ویژگی‌های اولیه‌ی دیوایس:

- در ابتدای کار دیوایس خود را با نام PUT و با BLEAddress برابر با 66:55:44:33:22:11 ادورتایز می‌کند.
- پس از اتصال موبایل به دیوایس، بعد از ۵ ثانیه به طور خودکار، دیوایس ارتباط را قطع می‌کند.

Services and Characteristics:

- دیوایس در لایه‌ی GATT، دارای سه سرویس است که درون سومین آن‌ها، چهار characteristic تعریف شده است. (از این به بعد برای اشاره به characteristic از کلمه‌ی کاراکتر استفاده می‌کنیم)

- **کاراکتر اول** که اجازه‌ی write را به اپلیکیشن موبایل می‌دهد، برای صحبت کردن با دیوایس است. تمام پیام‌هایی که بناست به هر شکل رمزشده یا نشده برای دیوایس ارسال شوند، در این کاراکتر نوشته می‌شوند.

- **کاراکتر دوم** که اجازه‌ی notify دارد به‌گونه‌ای است که پس از فعال شدن notify توسط موبایل، هر تغییری در محتوای خود را که توسط دیوایس داده شود، به اطلاع موبایل می‌رساند و موبایل باید در این زمان این کاراکتر را بخواند. (لازم است در ابتدای وصل‌شدن موبایل به دیوایس ، پارامتر notify مربوط به این کاراکتر توسط اپلیکیشن موبایل فعال شود.)

جریان ارتباطی:

- برای رمزنگاری از الگوریتم AES-128 استفاده شده است.
- در توضیحات زیر، عبارت AES(Plaintext, PrivateKey) به معنای آنست‌که عبارت ۱۶ بایتی Plaintext به عنوان ورودی، با استفاده از کلید PrivateKey و مطابق الگوریتم AES رمز شده است.

- **فعال کردن notify توسط موبایل**: بعد از وصل شدن به دستگاه، ابتدا باید در attribute مربوط به notify کاراکتر اول، این ویژگی فعال شود.
- **ارسال عدد رندم رمزشده برای موبایل برای اطمینان از اینکه موبایل به سرور متصل است**: سپس دیوایس در کاراکتر دوم خود، یک عبارت ۱۶ بایتی را notify می‌کند. این عبارت به شکل زیر است:

AES (data + rand, PRIVATE_KEY)

بدین معنا که ورودی تابع AES عبارتی ۱۶ بایتی است که ۱۲ بایت اول آن برابر data و ۴ بایت دوم آن برابر rand است که عددی رندم می‌باشد.

data شامل مبلغ تراکنش است. به عنوان مثال مبلغ ۱۱۰۰۰ریال به این صورت است:

data=”0x000000011000”

کلید خصوصی (PRIVATE_KEY) هم برابر عدد زیر است:

PRIVATE_KEY=”0x348572923FACE987CDD878614AA934B1”

- **ارسال عدد رندم گرفته شده از دیوایس برای سرور توسط موبایل**: موبایل عبارت دریافتی را به همراه ID دیوایس و همچنین درخواست تراکنش مالی، برای سرور ارسال می کند.

- **سرور از طریق زیر مطمئن می‌شود که دیوایسی که موبایل به آن متصل گشته، PrivateKey را در اختیار دارد و این به‌معنای authenticated بودن دیوایس است**:

سرور پس از دریافت پیام از موبایل، ابتدا باید با توجه به ID دیوایسی که موبایل به آن متصل شده است، PrivateKey مربوط به آن دیوایس را در حافظه‌ی خودش جستجو کند. سپس پیام مربوط به دیوایس را با استفاده از این کلید، رمزگشایی نماید. در صورتیکه فرمت پیام رمزگشایی شده به شکل مورد انتظار بود، دیوایس از نظر سرور authenticated تلقی می‌گردد.

- **ارسال پیام تأیید از طرف سرور برای موبایل:** سرور در صورت مورد تأیید بودن تراکنش مالی، تاییدیه‌ی زیر را برای موبایل می‌فرستد.

AES (rand + data PRIVATE_KEY)

- موبایل هم پیام دریافتی بالا را به دیوایس تحویل می‌دهد.
- **دیوایس از طریق زیر مطمئن می‌شود که موبایل به سرور متصل است و این به‌معنای authenticated بودن موبایل است. همچنین اطمینان از تأیید شدن تراکنش مالی توسط سرور نیز به‌طریق زیر صورت می‌پذیرد:** دیوایس پس از رمزگشایی و بررسی یکسان بودن عدد rand موجود در پیام دریافتی با عدد rand تولید شده توسط خود، بوق می‌زند.
- **دیوایس به موبایل اعلام می‌کند که پیام دریافتی مورد تأیید بوده است:** دیوایس عبارت زیر را در کاراکتر دوم، notify می‌کند:

“0x7061796d656e74446f6e65”

(معادل کد ascii این عبارت برابر است با paymentDone)

- **موبایل به سرور اعلام می‌کند که ارتباط موفقی با دیوایس برقرار کرده است. همچنین به دیوایس هم اعلام می‌کند که پیام اخیرش را دریافت نموده است:** موبایل با دریافت عبارت بالا، عبارت زیر را برای سرور و دیوایس ارسال می‌کند:

“0x5375636365737366756c”

(معادل کد ascii این عبارت برابر است با Successful)

- دیوایس با دریافت عبارت بالا، ارتباط را قطع می‌کند.