ارسال پیام دریافتی کاربر به اکسترنال CP

نسخه ۱,۴,۰,۰

تاریخ : ۹۶/۰۵/۲۹

برای ارتباط با سامانه‌ی پیام‌رسان اپسان باید یک API روی پروتکل HTTP به صورت زیر وجود داشته باشد.

Verb: POST

Input:

Message	String	Message sent to messaging system from end-user
Muid	String	UniqueCode For Message
FormattedMessage	String	Message that be formatted by aggregator
AccountId	String	User’s account ID
RecieveDate	DateTime	Timestamp in which the message is received by the system (UTC)
Operator	string	Currently available as MCI, IMI, MTN, RIGHTEL,
SID	string	the service identifier code provided by aggregator to third-party

در صورتی که متقاضی دریافت شماره کاربر هستندinput، مقادیر زیر نیز ارسال می گردد:

PhoneNumber	String	User’s Phone Number

این ورودی‌ها باید طبق استاندارد REST و در قالب یک JSON Object در Request Body قرار داشته باشند.

آدرس API فوق متعاقباً باید برای اعمال در سیستم در اختیار اپسان قرار گیرد.

پس از دریافت پیام از طرف کاربر، سامانه‌ی پیام‌رسان اپسان اطلاعات زیر را در اختیار آن نهاد قرار می‌دهد.

http request header:

appson-messaging-signature	امضای دیجیتال سامانه برای احراز هویت و اثبات صحت پیام ارسالی
appson-messaging-message	پیام ارسالی به آن شرکت با ساختار JSON برای اعتبارسنجی با امضای دیجیتال

http request body:

an object in above format

به منظور ارسال پیامی در جواب کاربر، آن نهاد می‌باید در پاسخ فراخوانی سرویس مذکور جوابی با ساختار زیر ارائه کند:

Signature	**String**	**External CP's signature**
Content	String	Content to be sent to the end-user (optional)
ContentType	Integer	Content's type. A number from Content Type List. See below.

Content Type List	
0	Default Message
1	Welcome message
2	Off Message
3	Help Message
4	Additional Help Message
5	Additional Default Message
6	Default Free Message

مقدار content این جواب باید با یک کلید نامتقارن (Asymmetric Key) امضا و **کلید عمومی آن (در فرمت XML) در اختیار اپسان قرار گیرد.**

برای اینکه آن شرکت بتواند پیام دریافتی از سامانه‌ی پیام‌رسان اپسان را در اختیار سامانه‌ی پیکو (سامانه‌ی پرداخت اپسان) قرار دهد باید مقادیر موجود در header پیام ارسالی را نیز در ساختار ارسالی خود به سیستم پیکو ارسال کند.

در اخر ادرس API ساخته شده در اختیار شرکت اپسان قرار گیرد.

پیوست ۱:

نحوه sign کردن اپسان

الگوریتم مورد استفاده برای **asymmetric cryptography**، الگوریتم RSA است که الگوریتم hash آن نیز SH1 است نمونه کد در زیر آمده است.

```
public static string Sign(string key, string text)
        {
            try
            {
                // Select target CSP
                var cspParams = new CspParameters { ProviderType = 1 };
                // PROV_RSA_FULL
                //cspParams.ProviderName; // CSP name
                var rsaProvider = new RSACryptoServiceProvider(cspParams);

                // Import public key
                rsaProvider.FromXmlString(key);

                // Encrypt plain text
                var plainBytes = Encoding.UTF8.GetBytes(text);

                var encryptedBytes = rsaProvider.SignData(plainBytes, new SHA1CryptoS-
erviceProvider());

                return Convert.ToBase64String(encryptedBytes);

                // Write encrypted text to file
            }
            catch (Exception exception)
            {
                Log.Error(exception.Message, exception);
                return null;
            }
        }
```