Security

Contents

1. Secure Access

Where at all possible you should use secure connections when using the API, particularly when usernames and passwords (or tokens) are being communicated across the internet or when messages contain sensitive information.

SSL or TLS can be used with HTTP (simple) and HTTP (sophisticated) APIs to secure access to our services. Similarly VPN connections can be put in place for this purpose.

2. Message Confidentiality

While SMS is a suitable means for communicating some sensitive information, it is not suitable for messages that absolutely must not be visible to parties that may lie between your application and the intended recipient. Where strong end-to-end encryption of SMS message content is used then SMS has as good message confidentiality as any other transport, however where available IP may be a more suitable than SMS.

3. Recommendations

For the HTTP APIs always use HTTPS with the HTTP (simple) and HTTP (sophisticated) APIs. For the SMPP API we recommend the use of TLS.

For SMTP (simple), SMTP (sophisticated) and non-TLS protected SMPP APIs we recommend the use of VPN connections. Contact Support or your Account Manager if you wish to have a VPN connection set-up.