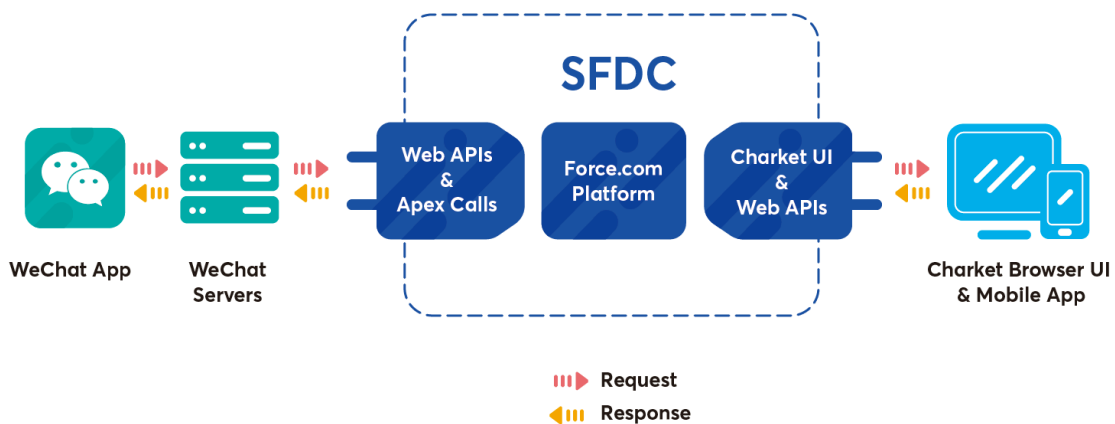


Charket Data Security

Data security is what we cared the most when we were designing our Charket app. Charket protects a customer's data by not storing any data outside the customer's own Salesforce org. Charket is a Salesforce native app that connects WeChat into Salesforce directly without having any servers in between. Charket is the most secure WeChat solution on the market.

The diagram below shows how a request and its response are routed across all points throughout the entire communication process.



Here are more details on how data is secured between any two points.

1. When a WeChat user initiates a request such as a message, a menu click, etc., the request first goes from the user's WeChat app to WeChat servers. The request in this case is encrypted by WeChat. This means even if a WeChat user's Internet connection is compromised, there is no way the data can be compromised. Below is a quote from WeChat's help center on how WeChat secures sent/received messages. This knowledge base article can be found at [this link](#).

WeChat securely encrypts your sent and received messages between our servers and your device ensuring that third parties cannot snoop on your messages as they are being delivered over the internet. We do not permanently retain the content of any messages on our servers whether they are text, audio or rich media files such as photos, Sights or documents. Once all intended recipients have received your message, WeChat deletes the content of the message on our servers and therefore third parties including WeChat itself are unable to view the content of your message. To ensure the privacy of your messages, it's important to make sure that you follow some safety tips. Read [more](#) about how to best secure your WeChat experience on all of your devices.

In some cases, you may choose to have your message content either saved to the server or

handled by a third-party service partner. For instance, when you select to add a message to Favorites, your message content will be automatically saved to our servers so that the message is available from within Favorites on any device that you log in to via WeChat. You may at any time de-select any message content from Favorites and they will be deleted from our servers. When you long-press a message and select Translate, the message may be translated via a third-party translation service, but the third-party shall not store the content of the message.

2. After receiving the request, WeChat servers forward the request to Salesforce. The request while being transmitted to Salesforce is encrypted using a TLS 1.2 or above certificate. The request is secure not just because it's encrypted but also it's transmitted between two data centers. It's very hard, if not impossible, to intercept such communication.
3. Salesforce stores data from the request and then forwards the request to an agent's browser or Charket mobile app. The request in this case is encrypted by Salesforce's TLS certificate. Salesforce is well known for its data security record.
4. When the agent's response goes back to the WeChat user, it goes through the same route but in the opposite direction. The returned response is secured the same way as how the received request is secured.

Salesforce disabled TLS 1.1 in October 2019. All data inbound to and outbound from Salesforce is encrypted using TLS 1.2 or above certificates which are considered safe and strong today and will take infinite resources to compromise.

Want to know more about Charket Data Security? Follow Charket by scanning the QR code on the right and chat with our technical experts.

