Sandes

Confidential Messaging as a Service (CMaaS)

A technical white paper on confidential messaging solution from Sandes Platform

January-2022

Abstract

Government Instant Messaging System provides instant messaging services to the government. Confidentiality is built in to the Sandes platform with the implementation of end-to-end encryption across all instant messaging services. This whitepaper focusses on the solution for end-to-end encryption between existing e-governance apps and users. The end-to-end encryption capabilities of Sandes platform is extended to existing applications, by offering a new class of cloud-based service called "Confidential Messaging as a Service" or CMaaS.

Prepared By	Reviewed & Approved By
Arun K Varghese Scientist C NIC, Kerala State Centre	Manoj P A Scientist F NIC, Kerala State Centre

Contents

Sandes

Background

Confidential messaging is a key government requirement to be addressed by ICT systems. At present, we lack a standardized, effective, and easy-to-use ICT system for confidential messaging within government. However confidential messages continue to be exchanged through various methods. The following are some of the existing confidential messaging scenarios:

Printed and delivered by hand

The most common manual method for securely sharing a top-secret, classified, or confidential information. This method is effective when the message is shared with limited receivers in geographically closer proximity. The method shall at times result in a huge waste of resources to ensure the intended guarantee of confidentiality.

Sending OTP as part of two-factor authentication

An OTP is generated by an application for two-factor authentication of a user. The two most popular modes for OTP delivery are SMS and email. In both SMS and email, the OTP message is transmitted in plain text. SMS in telecom networks are highly vulnerable[1] and poses serious threat to confidential messages. Moreover, SMS delivery is not free and are chargeable based on their delivery QoS. Email based delivery of OTP also suffer from QoS issues and was unsuccessful in adoption of PGP[2].

Password protection/Encryption

Password protecting a zip archive, PDF or document is another common technique to ensure confidentiality. These techniques internally use encryption and are effective in ensuring confidentiality. The only drawback is that there are no proper best practices or infrastructure to share the encryption password with the receiver.

[1] https://www.riverpublishers.com/journal/journal_articles/RP_Journal_2245-800X_512.pdf

[2] https://efail.de/

How does Sandes platform provide confidentiality?

End-to-end encryption is integrated to the core of the Sandes platform and provides confidentiality to its users across scenarios as given below:

1. One-to-one message exchanged between Sandes users are end-to-end encrypted
2. Group messaging is secured with end-to-end encryption
3. Messages exchanged between the Sandes Web app and Sandes mobile app are end-to-end encrypted
4. Messages pushed to a Sandes user by an external application through the Sandes gateway can be end-to-end encrypted

What is End-to-end encryption?

End-to-end encryption is an encryption scheme in which public-key cryptography is used by two communicating users to independently arrive on a common secret for encryption. The common secret is used by the sender for encryption of the message and by the receiver for decryption of the message. Apart from the basic functionality, the end-to-end encryption also implements a secure scheme to randomize the shared encryption to ensure that a different key is used for encryption of every message exchanged. This can ensure perfect forward secrecy for all communications.

Confidential Messaging as a Service (CMaaS)

Confidential Messaging as a Service is a cloud based confidential messaging solution offered to e-governance applications using Sandes platform.

Key Features

- ★ Confidential message and file sharing using end-to-end encryption
- ★ Message integrity check to prevent impersonation or message tampering
- ★ Message prioritization to ensure delivery QoS
- ★ Gateway Client service for quick integration
- ★ Auto rate limiting based on rate limiting plan to ensure high availability
- ★ Dispatched, delivery and read receipt for message requests

- ★ Support for runtime configuration change of rate limiting and IP whitelisting

Components

CMaas service is provided with the help of multiple components of Sandes platform. The key components are given below:

Sandes Messaging Gateway – A gateway service hosted by the Sandes platform that receives messages from registered app accounts and instantly delivers them to the Sandes app of the receiver.

Sandes Gateway Client Service – A light weight client helper service for the Sandes messaging gateway that is deployed alongside the application server of a registered external app. This service communicates to the gateway on behalf of the external app and transparently handles the end-to-end encryption at the message source. The integrating application is decoupled from the complexity of implementing the E2EE scheme and allows for a quick integration of confidential messaging. The gateway client service supports deployment in both Linux and Windows platform.

Sandes Instant Messaging Server – The Sandes instant messaging server shall be responsible to receive the confidential message from the messaging gateway and delivering to the Sandes app.

Sandes Mobile App – The confidential messages are received by the Sandes client app of the user and decrypted to show the plain message.

Confidential Messaging Process

The objective of confidential messaging process is to ensure that the messages and files are end-to-end encrypted between the sending application and the receiving user. Even a man-in-the-middle attack at any point in the communication channel should fail in breaking the confidentiality of the message. Confidential messaging process can be explained in four stages:

App account registration

An application must initially register for an app account to allow integration with the Sandes gateway messaging services. The account shall be whitelisted only for requests from a predefined set of white listed IPs. A client ID, client secret and HMAC key shall also be provided as part of the app account.

Publishing of user public key

- Sandes app creates an Elliptic Curve public/private key pair for the user device during initial login in the device
- User public key gets published using the Sandes APIs and the private key is secretly stored within the device key store

Configuration of gateway client service

The gateway client service shall be deployed in application server to run internally. The client ID, client secret and HMAC keys are also updated in the configuration. This enables the client service to integrate and communicate with the Sandes messaging gateway.

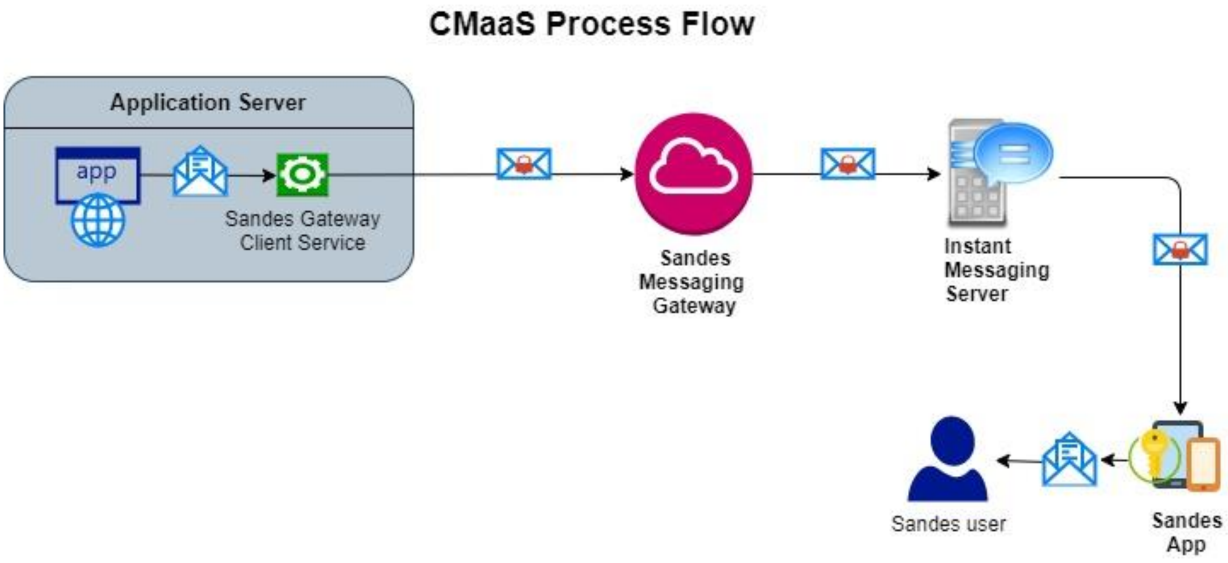
Sending a confidential message

- Gateway client service to generates an end-to-end encrypted message (confidential message) along with the identification of recipient (email or mobile)
- Confidential message is submitted to the gateway for delivery
- Message Gateway resolves the Jabber ID of the recipient from mobile and email and submits to the instant messaging server for delivery

Receiving a confidential message

- Confidential message is delivered to the recipient
- Confidential message/file gets decrypted by Sandes client and is displayed to the user

The following diagram shows a complete process of confidential messaging:



Secure OTP Delivery using CMaaS

One-time passwords are the most common use case that require confidential messaging. Hence, secure OTP delivery is the most suitable application for CMaaS.

OTP delivery should satisfy the following constraints of security, availability, and cost effectiveness:

Must use a confidential delivery mechanism to prevent man-in-the middle attacks

Confidential delivery is the most important and ignored aspect in OTP delivery. An OTP delivered over insecure SS7 networks are highly vulnerable to SMS hijacking attacks. OTP can only be secured by integrating with CMaaS which provides end-to-end support for encryption.

Must be delivered over a channel different from the first factor authentication

A breach in the system providing the first factor authentication (username/password) must not impact the second factor of authentication (OTP). Using Sandes gateway for secure OTP or even an SMS OTP can ensure compliance of this security constraint. For example, a user can receive secure OTP in Sandes for Parichay SSO which can be used for integrating other application.

OTP with short expiry require a high priority QoS for delivery

OTPs with short expiry requires a delivery channel that can ensure high priority QoS for timely delivery. Sandes gateway has inbuilt support for message prioritization to ensure that OTP messages are delivered on high priority. High priority SMS gateway requires services from multiple providers and shall have a fixed delivery charge per message.

Should be cost effective to support two factor authentications on a large scale

SMS based OTP is insecure at the same time not a cost-effective solution for two-factor authentication at a large scale. CMaaS offered by Sandes platform is the viable alternate solution.