SYMPHONY

June 2025

Contemporary digital communications:

A review of the solution landscape

Jérôme Folli, Kévin Renaudon, Mitch Hibbs and Olivier Richaud

This white paper examines the security and compliance challenges inherent in contemporary digital communications and compares and contrasts the approaches of various messaging solutions. While standard solutions often prioritize compliance, they often lack robust end-to-end encryption. Purely end-to-end encrypted solutions offer strong data confidentiality but pose compliance issues.

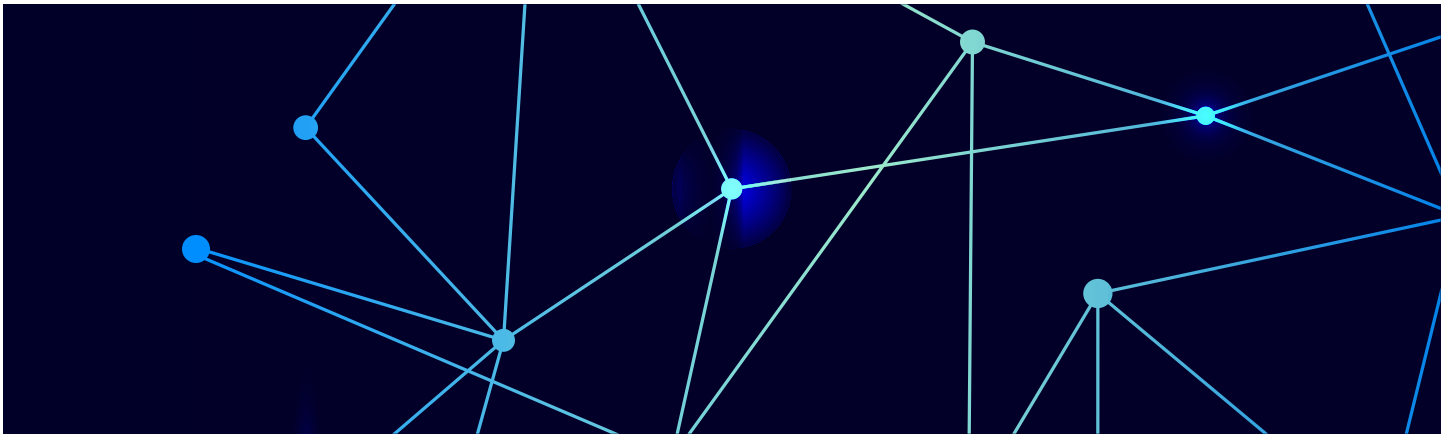
The Symphony Messaging platform specifically addresses both confidentiality and the need to comply with regulatory regimes. This document details Symphony's architecture, including its distinctive "cryptographic isolation protocol."

The protocol enables end-to-end encryption alongside comprehensive access controls and compliance capabilities, thereby demonstrating the suitability of Symphony Messaging for organizations with stringent security and regulatory requirements.

The messaging solutions landscape

The current digital environment provides organizations with a range of messaging solutions, each characterized by varying levels of security and compliance capabilities. This has become particularly prominent as people add messaging apps to their personal and professional workflows as a complement to e-mail.

That said, a thorough understanding of the differences between these solutions is crucial for selecting the appropriate platform for secured and regulated communications. This paper delves into three primary solutions categories: standard messaging, end-to-end encrypted (E2EE) messaging, and the unique approach offered by the Symphony Messaging platform.



1 Standard messaging solutions

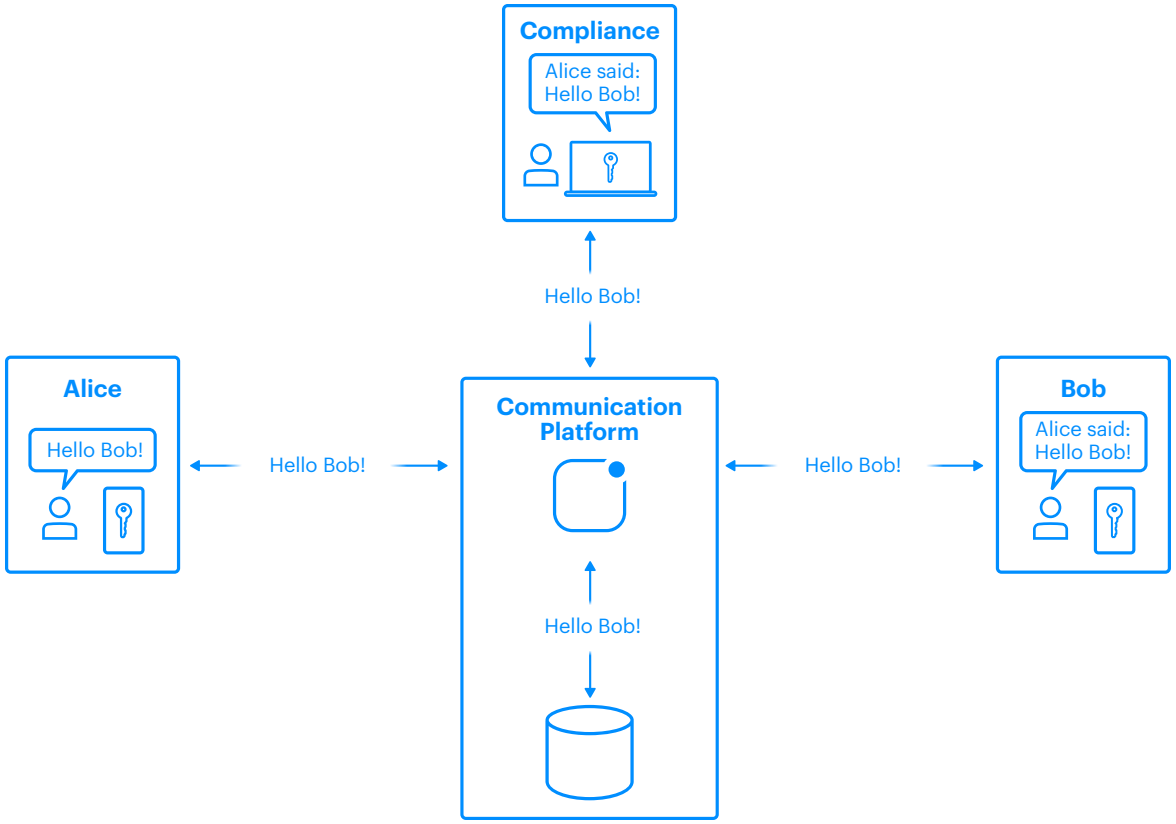


Fig. 1: Standard messaging solution

Standard messaging solutions typically employ in-transit encryption (such as Transport Layer Security "TLS") and at-rest encryption to ensure security and confidentiality of the data. In this model, data is often processed within the platform's backend infrastructure in an unencrypted state to allow certain platform functionalities like the ability to search messages.

While this architecture provides operational flexibility, especially for data processing subsystems, it introduces potential privacy vulnerabilities. Organizations are required to place trust in the messaging platform and the entities responsible for its management, which can lead to a perceived or actual loss of control and an elevated risk of data breaches.

A common mitigation strategy involves the use of customer-managed encryption keys to protect data at rest. But while this may restrict direct access to data at rest, it does not address the fundamental issue of data confidentiality, as sensitive information may still be processed by the messaging platform servers in plaintext.

2 End-to-end encrypted messaging solutions

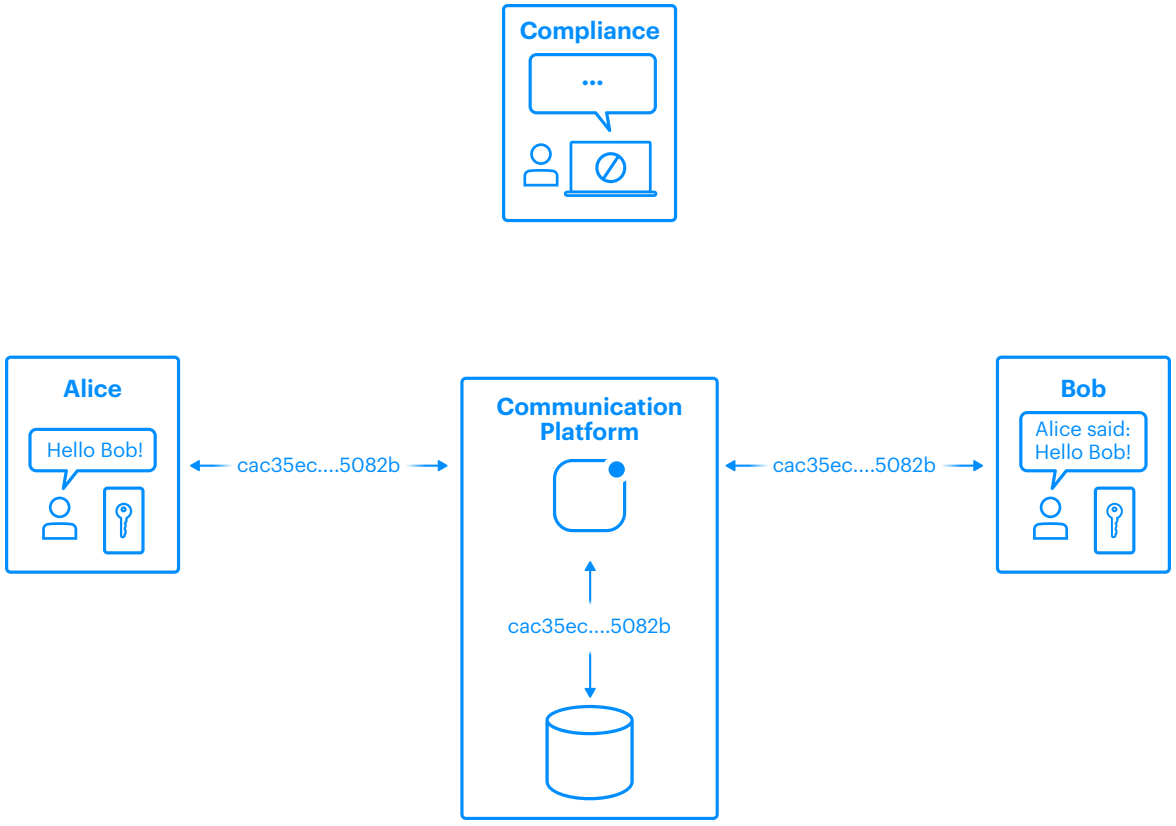


Fig. 2: End-to-end encryption (E2EE) messaging solution

End-to-end encrypted messaging solutions provide high levels of confidentiality by encrypting and decrypting data directly on the devices of the sending and receiving users. This ensures that even if the contents of a message are externally leaked or accessed without authorization, they remain inaccessible due to the inability to decrypt them.

This high level of confidentiality can pose challenges for compliance and auditing in regulated industries, such as financial services or healthcare. Given that encrypted messages are inaccessible to all parties except the sender and receiver, it becomes difficult for third parties, including regulatory bodies and internal governance teams to exercise oversight.

Additionally, unless strict controls are in place to authorize invited individuals, there is a risk of unauthorized individuals inadvertently or intentionally joining the conversation. Organizations must therefore carefully balance the privacy benefits of E2EE with the potential compliance, audit, and regulatory oversight challenges it creates.

3 Symphony's security and compliance model

Symphony's encryption

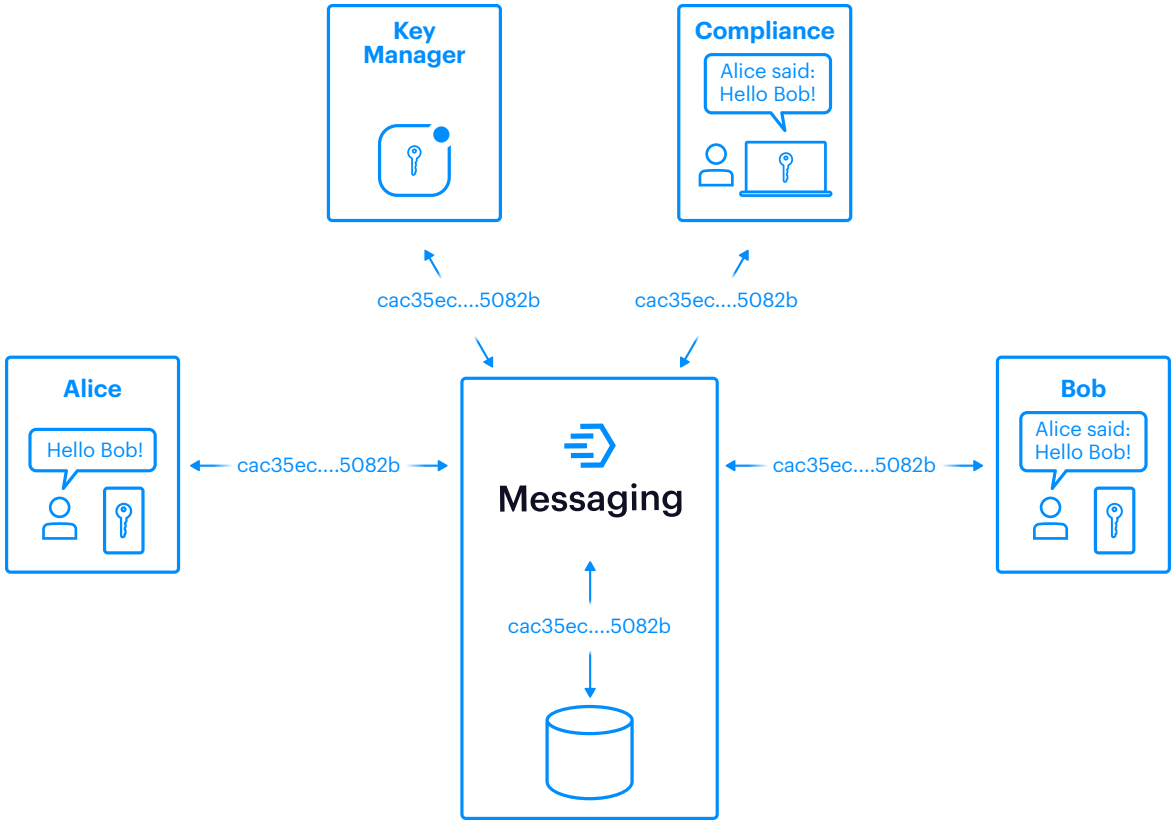


Fig. 3: Symphony's encryption using patented cryptographic isolation protocol

Symphony Messaging leverages end-to-end encryption natively for all messages and attachments transmitted in any type of conversation, including instant chats, rooms, large rooms, and even external conversations (inter-firm flows).

This ensures that neither Symphony nor its subprocessors (e.g. cloud service providers or managed service providers) can access data, as they lack access to the encryption keys.

In contrast to traditional E2EE messaging platforms, conversation encryption keys are not agreed upon between the different participants. Instead, they are computed in Symphony's Key Manager (which is under the control of the Symphony customer, not Symphony) using Symphony's patented cryptographic isolation protocol. Encryption keys are then securely exchanged between Symphony's Key Manager and all authorized participants, which employs a key encapsulation mechanism that ensures encryption keys remain perpetually inaccessible to Symphony.

This approach empowers Symphony's customers to:

Maintain control of their data: Symphony offers integration with customer-managed key management systems (hardware security modules), ensuring the tenant master key is always under the customer's control. Revoking access to those systems and keys will, for example, automatically crypto-lock the application, making it impossible for anyone to access data. When the keys are controlled, the data is controlled.

Facilitate compliance: In regulated organizations, it is mandatory to provide mechanisms for third parties to access data for oversight. Symphony enables compliance by exposing domain-specific privileges and roles, allowing specific users and systems to oversee data and events in the platform.

Minimize data exposure: Room encryption keys in Symphony Messaging are always shared with room participants with an additional layer of user-specific encryption applied to the keys. This ensures that even if a room encryption key leaks, only the authorized audience can decrypt it for use. This mechanism provides fine-grained cryptographic isolation, where each room is secured by its unique key, limiting access exclusively to the intended participants. Symphony also supports data protection solutions, including integration with data loss prevention (DLP) systems and malware scanners.

Control how encryption keys are distributed: Symphony's fine-grained access control model ensures that only intended users and systems can access chat content.

Trusted directory

Symphony Directory, a trusted network of market participants, is continuously updated by our customers to reflect the most current market user directory. Accessible across Symphony's Messaging and Voice platforms, the directory utilizes rich APIs and solutions that enable organizations to synchronize their internal directories with Symphony's global directory.

Companies and individual users can customize their directory information by adding details such as the user's specialization like asset class coverage and job function. This ensures that users can efficiently find and communicate with the appropriate individuals, all while employing end-to-end encryption.

Symphony Directory also provides robust and granular access management, preventing users from being unintentionally or maliciously added. Only authorized processes can update the directory, ensuring only the right audience can access sensitive data.

Communication controls

Symphony Messaging offers a wide range of communication control features that allow organizations to manage and restrict their users' network access to minimize the risk of data leakage. These include:

Granular privileges and user entitlements ensure that only authorized users can participate in external conversations.

Room visibility (one-to-one, internal, external, multilateral and federated), **connection request flows** and **room settings** significantly reduce the likelihood of accidental data leaks caused by potentially unauthorized individuals joining conversations.

Information barriers offer fine-grain tuning of communication flows within the same organization by allowing administrators to define and manage which groups of users are allowed to communicate with each other.

Private external communities allow external organizations to be onboarded privately. These communities are only accessible from the sponsoring organization and are not visible to the rest of the Symphony network. Additionally, Symphony Messaging can be integrated directly into a third-party application using Symphony's Embedded Mode, providing a native experience for those communities.

Federation (connectivity with external messaging systems) allows organizations to communicate with contacts in popular communication channels such as WhatsApp, SMS, Line and WeChat, while remaining invisible to the rest of the Symphony Messaging community. This allows organizations to conduct their governance and regulatory oversight responsibilities in these external platforms.

Compliance

Symphony provides a comprehensive set of tools to enable organizations to meet compliance requirements. This includes support for regular export of conversation data for integration with archiving solutions, room surveillance, and robust audit trails, allowing compliance teams to trace user actions.

The Symphony difference

The Symphony Messaging platform distinguishes itself by offering a unique architecture that integrates both end-to-end encryption and comprehensive compliance capabilities. Through its implementation of a “cryptographic isolation protocol”, Symphony ensures that data is encrypted and accessible only to authorized participants, while simultaneously allowing the necessary governance controls for regulatory compliance. This distinctive approach addresses the limitations of both standard and purely end-to-end encrypted solutions, providing a robust platform for organizations with stringent security and compliance requirements[1].

The Symphony Messaging platform is a solution that effectively balances the need for data confidentiality with the imperative of regulatory oversight, making it particularly suitable for industries and organizations where secure and compliant communication is paramount.

References

[1] FAQ Secure and Compliant Communications

Learn more at symphony.com or contact sales@symphony.com

Disclaimer

Neither Symphony Communication Services, LLC (together with its affiliates, "Symphony") nor the services which Symphony offers to its customers ("Symphony Services") is subject to the oversight or jurisdiction of any financial regulatory body.

Symphony is not, and shall not be construed as, a registered broker-dealer, an underwriter of securities, an introducing broker, or an entity performing similar or other regulated functions. Similarly, Symphony is not registered as, or to be construed as, a multilateral facility (including but not limited to a SEF, MTF or OTF), trading venue, regulated market or exchange. Because Symphony does not act in these capacities, nor is Symphony registered to do so, any indication to the contrary in this document or in any other document provided to you by Symphony shall be interpreted to the maximum extent so as not to imply that Symphony is acting in such capacity (or in any other capacity that is subject to regulatory oversight or subject to a requirement to register with a financial regulator).

Any Symphony Service that permits customers to negotiate the terms of any financial instrument is offered, and only capable of being used, on a purely bilateral basis. Symphony has no role or involvement in the negotiation or arranging of any transactions in financial instruments nor in the introduction of counterparties to one another for purposes of entering into such transactions. The execution of any such transaction is solely as between the counterparties thereto, and Symphony does not perform any execution, clearing or settlement function for any financial instrument transaction. To the extent that any Symphony customer utilizes Symphony Services for purposes of negotiating financial instruments, it is solely the responsibility of such customer to comply with any regulatory requirements to which such customer, or such negotiation, may be subject.

Neither this document, nor the offering by Symphony, or use by any Symphony customer, of any Symphony Service, shall be construed as a solicitation, endorsement, offer or recommendation by Symphony to buy, sell or hold any financial instrument, or an offer to provide any investment advice or investment services to any person in any jurisdiction. Recipients of this document and users of all Symphony Services alone assume the responsibility of evaluating the merits and the risks associated with the use of the Symphony Services.

Symphony is not a provider of call bridging services or any other regulated telecommunications functionality, and Symphony serves solely as a sales agent or network manager, and not as a "reseller," in facilitating use of any regulated functions. Symphony is not responsible for originating PSTN voice calls from, and terminating calls to, users on its platform, and such functionality is provided by third-party service providers.

Furthermore, certain of the statements and terms contained in this document may be forward-looking and contain concepts, product ideas or functionalities that are not currently part of the Symphony Service suite, but are instead contemplated by Symphony to be offered to customers at a future date. There is no guarantee that any such functionality will be offered by Symphony, and until such time, if any, as a particular functionality is included in the Symphony Services pursuant to a contractual agreement between Symphony and the customer utilizing such functionality, the depiction of such concepts, ideas and functionalities shall be construed as forward-looking only.

Nothing in this document or in the license or operation of any Symphony Service constitutes a representation by Symphony that is contrary to the foregoing disclaimers.