

# Fortifying Your Financial Data Security

In today's digital world, the protection of financial data has never been more critical.

---

**Dietmar Fauser, Chief Information Officer**

**Mitch Hibbs, Chief Information Security Officer**

# Fortifying Your Financial Data Security

In today's digital world, the protection of financial data has never been more critical.

Recent events have underscored the pervasive danger posed by advanced cyber threats. We have seen very severe supply-chain attacks that highlight how even modern cloud infrastructure is vulnerable to sophisticated attacks.

As a result, all organizations should currently be reassessing existing security architectures and measures.

At Symphony, we established our company on the fundamental principles of data security and regulatory compliance. As such, we are committed to providing our clients with the cutting-edge technology tools they need to safeguard their most valuable asset – their data!

Unfortunately, cybersecurity is evolving faster now than ever before. The number of publicly reported vulnerabilities continues to grow dramatically, with an anticipated increase of [25% in 2024](#). Critical sources of vulnerability analysis such as NVD are facing backlogs and delays. Meanwhile, we are seeing increasingly elaborate tactics being deployed. Focused efforts are being made to exploit vulnerabilities in digital infrastructure, even at the heart of the biggest cloud service providers. This is why all organizations need to remain vigilant and proactive in preparing for these emerging and fast evolving threats. It is imperative that all firms work with providers who are transparent about their security architectures and potential risks.

## Purpose-Built

As a leading technology firm in financial services, Symphony is purpose-built for this. Our technology empowers and protects communication services, data exchanges and digital workflows within and across a wide variety of organizations. Our products are not only built with the highest cryptographic protection, but they are specifically designed to comply with regulatory controls, information barriers, auditability and data archiving.

With Symphony, you can safely build cross-firm workflows with confidence, knowing your data is not only protected at every step but also conforms with strict information security rules.

Additionally, we separate the application logic from the security layers, which offers greater flexibility in implementing new security features.



# Collaboration - With a Secure Audience

We firmly believe in fostering a culture of collaboration and transparency, especially when it comes to cybersecurity.

Symphony works closely with our clients and partners to understand their risks and regulatory requirements. This enables us to develop tailored solutions to address the unique needs of the financial services industry.

While many firms in our industry rely upon email in their daily business operation, we believe that email based communication is a high risk for unintentional data leakage. We also believe it is an inferior mechanism in targeting the right audience for various human assisted financial workflows.

At Symphony, we maintain a customer curated and enriched directory of 700,000 professionals across global finance. Our directory and membership allow our customers to communicate directly with the precise professional in charge of a given task. This eliminates the error-prone usage of email addresses that are often 'managed' in spreadsheets and quickly become outdated. We work hard to provide this community ways to communicate, collaborate and partner with security as a fundamental design tenet.

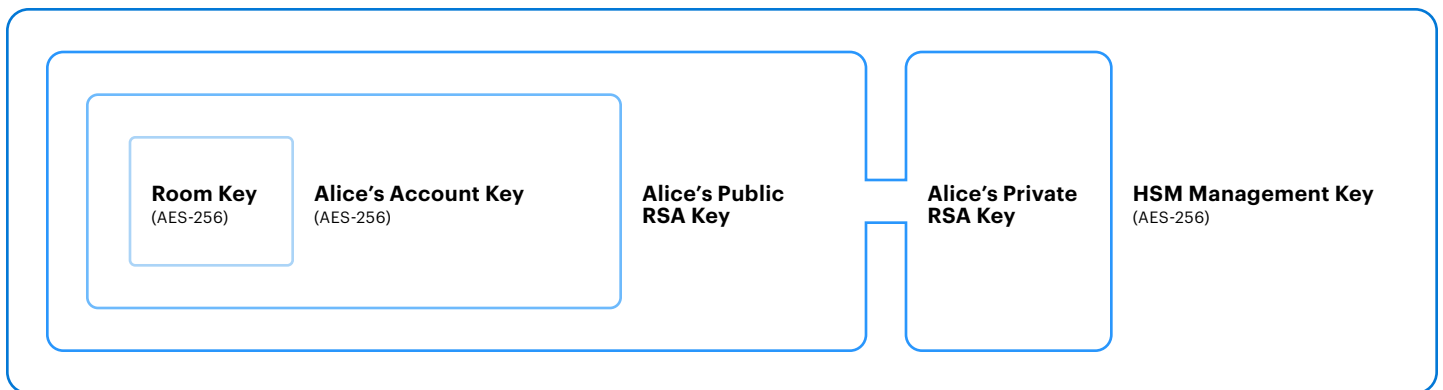
# Cryptographic Key Protection

Symphony offers the only cloud-based, secure, team collaboration solution that combines end-to-end encryption, borderless external and internal communication, and enterprise-class administration into a single, extensible platform. This provides reach, flexibility and protection to all involved parties.

We have built a state-of-the-art crypto system that is protected by patents, which incorporates a multi-layered, conversation specific, key architecture.

At Symphony, we have no concept of using a single key to access broad swaths of information. In our architecture, each chat room has its own encryption key and each individual user has their own encryption keys. Compartmentalization of encryption key scope radically reduces the surface area of risk-exposure.

A sophisticated key-wrapping approach is employed to protect and deliver keys to the endpoint.



Conceptual view of the Symphony encryption key hierarchy and wrapping approach

Fundamental features like key-expiry management and key-rotations are standard features. More importantly, these can all be initiated by customers directly and do not require manual emergency procedures. As an optional implementation, Symphony offers a full 'Bring Your Own Key' capability where the master keys are fully owned and managed by our customers.

That means they never leave the Hardware Security Modules (HSMs) deployed in their environments. These keys always remain in the HSMs, within the network domains of our customers, and are subject to customer's security team monitoring. Put simply, when you control your keys, you control the security of your data. No other approach is as effective... or as responsible.

# Future Threats

**We are currently seeing completely new threats arising.**

A growing area of industry concern is quantum computing which is why the term “Post Quantum Cryptography” is rapidly gaining popularity. The big question here is how long current crypto algorithms like RSA or AES will withstand the new computing capabilities of quantum computers. There is also the risk of large AI systems capable of ‘cracking’ the existing algorithms.

At Symphony we follow these evolutions very carefully to understand and test new algorithms as they become available. We are continually seeking new approaches that will be able to protect client data, even in a quantum computing environment. We work with partners and academia to be ready for these new challenges.

We do all this because we believe that there is a very large risk building - one that is currently not fully understood. The reality is that the massive amount of encrypted data archives will be subject in the future to attacks by a new generation of technology, specifically quantum computing and AI. Moving early here is critical to limiting the amount of archived data with outdated encryption schemes.

This is our focus.

There is a fundamental notion of ‘separation of concerns’ applied in the Symphony platform today. Essentially, we strictly separate application logic from the cryptographic layers and algorithms. This enables our engineering teams to ‘play’ with new algorithms easily and to implement them early, without deeper dependencies on the application logic.

As a result, we are able to constantly test and iterate on potential new development and protections. We are aware that most companies do not have the capability or toolsets to do this themselves, which is why we remain so committed to this as a discipline.

# Conclusion

Data security and regulatory controls grow more important every year. This is due to increasingly sophisticated hacking groups, generational shifts in technology, and the massive financial fines imposed by the regulators in cases of non-compliance with data-handling requirements. All of this results in a pressing need for robust data security.

At Symphony, we remain committed to empowering our clients with the tools and technologies needed to navigate today's complex cybersecurity challenges. We do this while offering modern communication tools, enabling digital workflows, and providing a large curated directory to the financial industry.

We know how much our clients rely upon us and our advanced toolsets.

By prioritizing cryptographic protection, offering purpose-built security solutions, and fostering a culture of collaboration and transparency, we stand as a trusted partner in safeguarding your financial data - both today and tomorrow.

## FURTHER READING AND RESOURCES

If you have additional additional questions or would like to continue the conversation, please connect with [Dietmar Fauser](#) or [Mitch Hibbs](#) on LinkedIn, or email [csso@symphony.com](mailto:csso@symphony.com)



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.

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.

**Learn more at [www.symphony.com](http://www.symphony.com)**  
**or contact [sales@symphony.com](mailto:sales@symphony.com) for more information**