

Case Study



Industry : Insurance
Solution Focus Area : Security

Swiss Re explores further protection of critical data using “Confidential Computing” – a proof of concept enabled by Decentriq’s Confidential Computing using Intel® Software Guard Extensions (Intel® SGX)

DECENTRIQ



Challenge

Today, Re-insurance enterprises expect big data to generate significant improvements to their marketing, client experience, underwriting and claims management. Re-Insurance enterprises such as Swiss Re that embraces a data analytics approach can use data for more accurate and meaningful insights from the ever-increasing amounts of data being generated from a variety of sources. For Swiss Re, one of the world’s largest reinsurance providers, data is key to understand and reinsure risks to make the world more resilient.

Confidential Computing and Decentriq

In today’s data centred world, data is normally encrypted at rest, in storage and in transit, but there is demand for protection of data in use to ensure that data is protected even while it is being processed. Enterprises and organisations that are working with sensitive data, such as Personally Identifiable Information (PII), financial data, or health information, need to mitigate threats that target the confidentiality and integrity of either the application or the data being processed. The sovereignty of customer data should be protected and not subject to attacks from external or internal threats. Although Swiss Re is a reinsurance leader known for leveraging data science and sophisticated machine learning models, gaining access to data sets that contain sensitive information continues to present significant challenges.

Confidential Computing, as made available by Decentriq, helps to protect data in use by performing computation in a hardware-based Trusted Execution Environment (TEE). These isolated environments also known as enclaves help to secure data, IP and code and to prevent unauthorized access or modification of applications and data while they are in use.

Confidential computing not only significantly improve the protection of data, it provides paths for companies to extract analytical, actionable insights from this data – whilst helping to maintain consumer privacy.

In a world where we are constantly storing, consuming and sharing sensitive data – from credit card data to medical records, from firewall configurations to our geolocation data – protecting sensitive data in all its states is more critical than ever. Cryptography is now commonly deployed to provide both data confidentiality (stopping unauthorized viewing) and data integrity (preventing or detecting unauthorized changes). While techniques to protect data in transit and at rest are now commonly deployed, the third state - protecting data in use - is the new frontier called Confidential Computing.

Decentriq’s Confidential Computing-based platform is built using Intel® Software Guard Extensions (Intel® SGX). Intel® SGX is one of the main technologies powering Confidential Computing today, enabling new cloud use cases such as Multi Party Computation, Privacy Preserving Machine Learning and many others spread across industries that are dealing with privacy and the cloud on a day-to-day basis. Intel® SGX is the most tested, researched, and deployed hardware based Trusted Execution Environment in the data centre with the smallest available attack surface within the system.

Decentriq's mission is to solve cloud security and privacy challenges, particularly for organizations collaborating on sensitive data both internally and externally. Decentriq technology allows customers to operate on even the most sensitive and private data sets without having to trust the cloud provider. Decentriq provides deterministic security by encrypting applications and data everywhere – at rest, in motion, and in use with its technology built upon Intel® SGX and other Intel security technologies.

Decentriq created its platform in 2019, one of the first SaaS solutions to implement confidential computing. Decentriq provides an innovative approach to security and privacy, allowing organizations with sensitive data to operate in the public cloud to exchange and collaborate on data with each other.

Intel® SGX offers hardware-based memory encryption that isolates specific application code and data in memory. Intel® SGX allows user-level code to allocate private regions of memory, called enclaves, which are designed to be protected from processes running at higher privilege levels. Only Intel® SGX offers such a granular level of control and protection.

Intel® SGX can help prevent against attacks such as memory bus snooping, memory tampering and cold boot attacks against memory in RAM. It helps protect against software-based attacks even if the operating system, drivers, BIOS and Virtual Machine Manager are compromised.

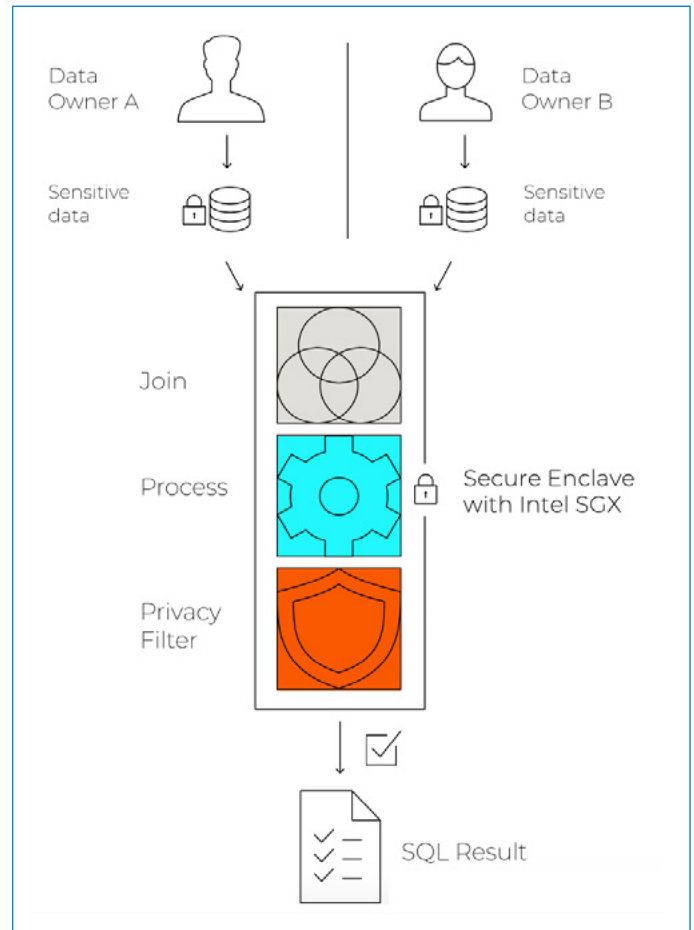
This data is no longer a tool that records what has been done, it's now a tool to fuel future growth. Swiss Re leverages its global footprint, deep understanding of insurance, ever increasing access to data and state of the art data science capabilities to equip their insurance clients across the globe with the right tools to drive actionable data insights. For Swiss Re's proprietary risk models and tools to become more efficient, they, amongst other things, use machine learning models to have constant access to new data sources. However, one of the challenges that the industry faces is doing analytics on critical data sources, while ensuring the data remains protected. These data sources can be highly relevant for assessing existing or new risks e.g. in the area of IoT, – by making them usable in a protected way, insurability, fair pricing and efficient claims processes can be enhanced or even enabled.

As a data-driven, risk knowledge company with a major focus on machine intelligence, Swiss Re constantly pursues initiatives to test new data driven technologies. Swiss Re recognizes the potential of doing analytics /while keeping the data protected, and therefore has launched multiple workstreams to explore new technologies in this field. Among this is Confidential Computing with Decentriq and Intel® SGX.

Swiss Re's collaboration with Decentriq is opening the door to Confidential Computing, by helping Swiss Re's machine learning algorithms.

Swiss Re & Decentriq – Collaborative Application in Marine Insurance Data

Swiss Re needs continuous data sets for marine shipping data from supply chain data aggregator platforms, but data privacy and competitive concerns present barriers in accessing that data. From an insurer's perspective, marine data is critical because the total value of goods in port at any point in time is calculated only up to a certain point. This presents difficulties for Swiss Re as building calculation models with incomplete data increases the risk of over- or underestimation. The goal of the pilot program with Decentriq was to demonstrate the data size scalability and security when processing confidential operations on marine data set by generating larger amounts of data synthetically.



In Swiss Re's evaluation of the Confidential Computing solution provided by Decentriq the focus was on several key areas:

Performance – Swiss Re found no performance degradation while using Decentriq's solution with typical data sets used by Swiss Re. With 3rd Generation Intel® Xeon® Scalable Processors, Swiss Re anticipates even further order of magnitude performance optimisation.

Time to Market – Swiss Re is confident that new use cases can be deployed with Decentriq technology in an expeditious manner thus increasing time to market and with reasonable development and run costs.

Security – Swiss Re solicited one of its preferred security advisors to run a security audit including penetration testing on the Decentriq solution which found no significant issues over a 3-day audit.

The successful collaboration has shown that Confidential Computing with Decentriq and Intel SGX is a technology that can solve issues and is ready for enterprise scale across a variety of use cases.

Closing Remarks

As the insurance industry evolves to an even more data driven service, one can see the concept of Insurance as a Service becoming a commodity seamlessly integrated along with other services. To achieve this, leading re/insurers could continue to build ecosystem partnerships with data providers and suppliers like Decentriq and Intel. Gaining access to sensitive data sets from sources that are trusted will be at the core of this new paradigm, helping to drive new business segments, personalised insurance, increased transparency into supply chains and more succinct insurance pricing models.

Confidential Computing powered by Intel® SGX technology delivered by Decentriq can help to continue to unlock data sources that were previously unattainable in real time. This important initiative allows organizations to continue to be driven by analytics while on a variety of data sets.

"As a data and technology driven risk knowledge company, Swiss Re intends to make use of confidential computing technologies. I'm optimistic that this will continue to allow Swiss Re to access and analyse data in new ways to help unlock new forms of value creation in risk protection today and in the future" said Sebastian Eckhardt, Expert Business Analyst at Swiss Re.



Performance varies by use, configuration and other factors. Learn more at www.intel.com/PerformanceIndex. No product or component can be absolutely secure. Your costs and results may vary.

Intel technologies may require enabled hardware, software or service activation.

Statements in this document that refer to future plans or expectations are forward-looking statements. These statements are based on current expectations and involve many risks and uncertainties that could cause actual results to differ materially from those expressed or implied in such statements. For more information on the factors that could cause actual results to differ materially, see our most recent earnings release and SEC filings at www.intc.com.

© Intel Corporation. Intel, the Intel logo, and other Intel marks are trademarks of Intel Corporation or its subsidiaries. Other names and brands may be claimed as the property of others.

About Swiss RE

The Swiss Re Group is one of the world's leading providers of reinsurance, insurance and other forms of insurance-based risk transfer, working to make the world more resilient. It anticipates and manages risk – from natural catastrophes to climate change, from ageing populations to cybercrime. The aim of the Swiss Re Group is to enable society to thrive and progress, creating new opportunities and solutions for its clients. Headquartered in Zurich, Switzerland, where it was founded in 1863, the Swiss Re Group operates through a network of around 80 offices globally. It is organised into three Business Units, each with a distinct strategy and set of objectives contributing to the Group's overall mission.

DECENTRIQ

About Decentriq

Decentriq is an enterprise SaaS platform providing data clean rooms - allowing users to leverage data previously not possible.

Easily and securely collaborate with stakeholders, internal or external, to derive new data value. Decentriq's underlying encryption-in-use technology utilizes Intel® Software Guard Extensions (Intel® SGX) which helps to protect data.

Decentriq is a founding member of the Confidential Computing Consortium