



SenSage / EMC

EU Data Retention Directive

Proof of Concept, FAQ

Frequently Asked Questions

EU DATA RETENTION DIRECTIVE	3
WHAT IS THE EU DATA RETENTION DIRECTIVE?	3
WHO MUST ADHERE TO THE DIRECTIVE?	3
WHEN DOES THE DIRECTIVE GO INTO EFFECT?	3
WHAT TYPE OF DATA IS TO BE RETAINED AND HOW SHOULD IT BE PROTECTED?	3
WHAT ARE THE DIRECTIVE ACCESS AND ANALYSIS REQUIREMENTS?	3
DON'T TELCOS AND ISPS SUPPORT AUTHORITIES TODAY?	3
PROOF-OF-CONCEPT (POC)	3
WHY DID SENSAGE AND EMC COLLABORATE ON A PROOF OF CONCEPT?	3
WHAT DO SENSAGE AND EMC BRING TO THE SOLUTION?	3
WHAT DOES THE JOINT SOLUTION DELIVER?	3
WHAT POC OBJECTIVES WERE MET?	4
WHERE DID THE DATA COME FROM AND HOW MUCH DATA WAS MANAGED?	4
WHAT BAR DOES THE POC SET?	4
WHAT IS THE VALUE OF THE JOINT SOLUTION COMPARED TO TRADITIONAL APPROACHES TO ADDRESS THE DIRECTIVE?	4
WHAT CAN BE LEARNED FROM THE POC ANALYSIS?	4
WHAT VENDORS CONTRIBUTED TO THE POC	4

EU Data Retention Directive

What is the EU Data Retention Directive?

The EU Data Retention Directive is a set of guidelines established March 2006 by EU member states that mandates Telcos and ISPs retain telephone, Internet access and messaging service transaction records for a period of time between six months and two years. Upon an authorised inquiry, the service provider must deliver appropriate data, without undue delay, based on searches against the retained data. The purpose of the Directive is to enable law enforcement agencies to expedite the identification, investigation and prosecution of person(s) involved in - crimes and terrorist activity.

Who must adhere to the Directive?

Telcos and ISPs offering fixed, mobile and Internet telephony, as well as Internet access, email and messaging services that operate in the 25 EU member countries. The initial phase of the Directive calls for Telcos to retain and be able to analyze Call Detail Records (CDR). Subsequently, the next phase of the Directive calls for Telcos and ISPs to retain and be able to analyze Internet and messaging transactions.

When does the Directive go into effect?

The Directive calls for member countries to establish and enact laws within their countries by September 2007. Each member country will determine the retention period and establish when each phase of the Directive guidelines go into effect for Telco and ISP providers.

What type of data is to be retained and how should it be protected?

The Directive indicates the name, user ID and address of the source, as well as the destination of the communication, the date and time the communication took place, the equipment used, and the geographic location involved be retained. The Directive guidelines refer to transaction details – not the actual content that transpired. The guidelines specify that segregated data storage be in place (it cannot be co-joined with business data processing), as well as setting appropriate access controls, data integrity and availability provisions. Privacy and data protection policies set by EU country members must also be preserved.

What are the Directive access and analysis requirements?

The Directive states that only authorised requests used for the purpose of law enforcement and the investigation of crimes including terrorism. The systems must not only retain the data, but must also provide timely results to authorities that meet the standard of “without undue delay.” Timely is defined as providing useful, relevant and pre-process transaction data in minutes – not hours or days.

Don't Telcos and ISPs support authorities today?

Telcos and ISPs do currently work with law enforcement authorities, however, this support varies by member country. Depending on the Telco and ISP and the member country in which they operate, the current provision will most likely not support the Directive guidelines. Generally speaking, Telcos and ISPs have not been required to store historical data and provide records of past activity. Nor has the response time to provide said transaction data been “without undue delay.”

Proof-of-Concept (POC)

Why did SenSage and EMC collaborate on a Proof of Concept?

The Directive places significant storage, security and analysis obligations on Telcos and ISPs. While Telcos and ISPs often support law enforcement, their systems may not currently meet Directive standards. Conventional transaction recording systems may be expanded to meet the Directive, but this would present material expenditures, as well as new operational and technical considerations. Therefore, SenSage and EMC collaborated on a Proof of Concept (POC) to demonstrate a more effective, lower cost EU Data Retention Directive solution offering lifecycle event data management, high-speed analysis, on-line retention and robust storage management capacity. Ultimately, the companies will offer this proven solution to help Telcos and ISPs support the Directive guidelines.

What do SenSage and EMC bring to the solution?

SenSage provides a proven, scalable event data management platform that optimizes the collection, management and analysis of massive, diverse volumes of event data. EMC provides a simple, scalable and secure storage solution for cost-effective retention, protection and disposition of fixed content. The combination delivers a cost effective, low maintenance solution for the Directive that can integrate with existing Telco and ISP transaction data mediation sources.

What does the joint solution deliver?

The joint SenSage / EMC POC, as collaborated by SenSage and EMC, offers European Telco's and ISP's a viable and cost-effective approach to address the mandated EU Data Retention Directive. It also enables law enforcement authorities to quickly access, investigate and prosecute terrorists and - crime activity derived from phone and Internet records.

What POC objectives were met?

The joint solution achieved the following objectives: (1) Retain and analyze over 100 Billion call detail records (CDR), (2) Produce answers to required queries in as little as 15 minutes against a real-world data set, (3) Deliver a cost effective approach with lower comparative Total Cost of Ownership (TCO), (4) Demonstrate that nominal administration is needed to operate (5) Maintain the solution, and demonstrate integration, management and expansion advantages which support Directive requirements.

Where did the data come from and how much data was managed?

With support from Intec Telecom Systems, SenSage and EMC legally obtained sample CDR data from a leading telecommunications provider. A data cleansing, randomization and replication application was built and applied to the original data set in order to generate the necessary volume. The data generation application produced more than 100 Billion records, which occupied over 13 TB of compressed, raw managed data.

What bar does the POC set?

While any Directive project can be achieved with unlimited funds and resources, the POC delivers a proven solution that meets the Directive requirements at significantly less total cost of ownership as compared to conventional approaches. The system simulated a two year retention period of actual CDR data of a Telco with 10 million subscribers (10 million unique call numbers) yielding 135 million calls per day. The sustained data load rate was 300,000 CDR insertions a second. The more than 13TB of CDR data stored on the system was the result of compressing the raw data by 50per cent ,-- yet the entire data set is available for analysis. The system queried approximately 30 million un-indexed records per second and delivered results to a three-month inquiry in less than seven minutes.

SenSage's patented event data management capabilities enable queries to be achieved at exceptional speed and without reliance on Relational Database Management System (RDBMS) technologies or RDBMS pre-computed or pre-defined indices. EMC Centera provides a high value storage solution with complete data integrity, protection and availability features. The entire system integrated with existing CDR mediation sources, could be managed as a segregated event data management solution, and leveraged low-cost, high performance servers and networking configurations.

What is the value of the joint solution compared to traditional approaches to address the Directive?

Alternative traditional approaches use a combination of existing mediation systems, storage and Relational Database Management System applications. RDBMS solutions are scalable and, with a significant investment in processing, system tuning, administration and storage resources, can be designed to manage CDRs to achieve desired Directive goals. Based on vendor research, it is estimated that the POC can deliver the functionality to support Directive requirements at approximately 15% of the cost of a fully loaded traditional system; this includes integration, design, tuning and storage consultancy, RDBMS licensing, labor resources and storage consumption. Furthermore, the joint solution is segregated and offers more convenient and economical storage and processing scalability.

What can be learned from the POC analysis?

The POC findings provide results that can be used for solution guidance. The POC queries simulated common law enforcement requests, such as retrieval of all calls made from a specific phone number, or all calls made between two specific phone numbers, during a defined period of time – against 100 billion call records. The POC load and retention rate is not an upper bound, but served to illustrate the performance achieved with the current configuration. Even greater load and retention rates can be achieved by adding additional SenSage nodes and EMC Centera nodes. Other factors beyond the scope of this POC, such as system configurations and tuning, would yield even greater performance and capacity results.

What vendors contributed to the POC

SenSage, EMC, Red Hat, Dell, Intel, Cisco and Intec contributed to achieving POC objectives. The solution is comprised of the SenSage scalable event log management and analysis platform. An EMC Centera Gen 4 Content Addressable Storage (CAS) system extends the overall POC data integrity, protection and availability. SenSage software was run on the latest RedHat 64-bit Linux platform installed on Dell PowerEdge 2950 Servers utilizing the new Dual-Core, Dual CPU Intel Xeon processors (aka Woodcrest). The POC components worked on a Gigabit network using the Cisco Catalyst 3750 high-speed switch. Intec Telecom Systems provided CDR mediation and solution guidance on the POC project.

© Copyright 2008 SenSage, Inc. All rights reserved. All names and marks used herein are the property of their respective owners.