Secure Long-term Record Keeping in the Public Sector

Lucie Langer I Alex Wiesmaier I Johannes Buchmann

abstract

Electronic government requires secure retention of sensitive documents over long periods of time, where conventional encryption methods cease to be effective. A recently completed project has come up with a trustworthy infrastructure, the "Lifetime eSafe", which provides a means to securely retain sensitive data in the public sector without relying on the security of cryptographic algorithms. Its follow-up project "CloudSafe" uses the potential of the cloud to further enhance the eSafe.

Secure Record Keeping in Public Administration. The spread of eGovernment brings along many benefits such as more convenience for citizens, improved access to information for both citizens and businesses, and increasing efficiency of services provided by the government. However, the implementation of eGovernment procedures also comes along with specific challenges such as secure record keeping.

Public administration requires secure retention of relevant documents in order to provide evidence of an activity or decision. But whereas confidential storage of paper documents can be achieved by putting them in an archive once and for all, secure long-term retention of electronic data is a more challenging task.

Apart from the requirements of integrity and authenticity, preserving the confidentiality of the documents requires specific measures. Electronic data can, for example, be encrypted in order to hide its contents. But this approach falls short in the long term: it is well known that the security of all practical cryptographic algorithms decreases over time. Thus, encrypted data can lose its confidentiality in the course of time. Since electronic records of eGovernment procedures usually must be kept for several years or even decades, other ways of ensuring confidentiality have to be found here.

Approach: Lifetime eSafe. The task of retaining sensitive data in the public sector requires a trustworthy storage unit which does not rely on conservative encryption and enables the user to deposit documents securely and confidentially in the long term. Such a storage unit, the "Lifetime eSafe", has been developed within a recent project conducted by a team of researchers from the Cryptography and Computer Algebra Group at Technische Universität Darmstadt in collaboration with the Lorenz-von-Stein Institute for Administrative Sciences at the University of Kiel.

The project has come up with a distributed architecture, the "Lifetime eSafe", which is run by a consortium of service providers (see Figure 1). Each record deposited in the eSafe remains confidential as long as the number of maliciously collaborating providers does not exceed a specific threshold. Each record is split into several shares, which are subsequently distributed among the service providers and stored by them. This approach was introduced in[(1)] and uses secret sharing according to Shamir[(2)]. Thus, confidentiality does not hinge on the security of encryption algorithms that may be broken in the future, which makes this approach particularly suitable for long-term storage of electronic records. Moreover, this decentralized storage concept enhances availability by avoiding a single point of failure: any (sufficiently large) subset of servers may be queried to provide a share in order to allow for reconstructing the document. This also allows for a reasonable load balancing, as the load can be distributed over various redundant servers.

The Lifetime eSafe can also be used as a secure storage unit within the Reference Architecture for Trustworthy Long-term Archiving proposed by the Federal Office for Information Security[(3)]. This directive regulates

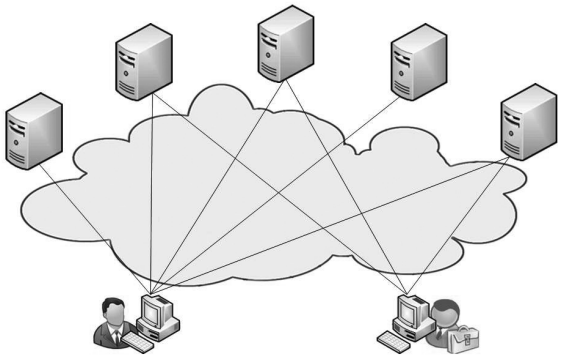

Fig. 1: Design of the Lifetime eSafe

trustworthy long-term archiving in German government agencies and supports the integrity and authenticity of archived data. By integrating the Lifetime eSafe into the Reference Architecture, confidentiality and availability can be achieved as well[4].

Application in eGovernment. The eSafe acts as a common data storage shared between the public administration and citizens or companies, or between several public offices who wish to securely exchange or to store data.

In a very simple example, public office A wants to keep long-term records of a certain eGovernment process conducted with citizen B. Instead of communicating directly, the parties communicate via the eSafe. This indirect communication is handled automatically and transparently by the communicating parties' software. The eSafe then automatically keeps the records of the communication in a way which is secure in the long term,

In the underlying technical layer, which is not visible for the parties involved, this example works as follows: B initiates the process by putting a completed form into the eSafe, and informing A on that fact. A then loads the form from the eSafe, processes it, puts it back into the eSafe and informs B on the completion of the process. B can now review the form and check the results.

Other, more complicated scenarios, possibly including more steps and communication partners, are conducted analogously. Depending on the rules defined, the eSafe automatically keeps all or part of the exchanged data in a way which is secure in the long term. There is no need for re-encryption or similar actions in order to maintain confidentiality. In case the data involves electronic signatures, these can be kept valid in the long term using the mechanisms defined by the Reference Architecture (3).

Current Work. Cloud services offer high scalability and high availability at a reasonable price, but suffer from lacking trust in existing data protection concepts. In the follow-up project "CloudSafe" we enhance the eSafe to become a verifiably secure infrastructure for processing and storing data within the cloud.

The core of the project is an electronic data safe which guarantees long-term confidentiality without relying on the trustworthiness of third parties. This allows for keeping sensitive data in private or even public clouds without relying on the security mechanisms of the cloud. Thus, the potential of cloud computing can be used while maintaining data protection.

The new concept preserves the availability and load-balancing capabilities inherited from the eSafe project, and additionally ensures long-term confidentiality during data transmission.

This gives the public sector the possibility to provide citizens, business partners, and customers with a trustworthy, highly scalable and highly available infrastructure without having to operate the necessary infrastructure themselves.

literatur

(1) Miyamoto, Toshiyuki; Doi, Shinji; Nogawa, Hiroki; Kumagai, Sadatoshi: Autonomous Distributed Secret Sharing Storage System, Systems and Computers in Japan, vol. 37, no. 6, 2008.

(2) Shamir, Adi: How to Share a Secret. Communications of the ACM, vol. 22, 1979.

(3) https://www.bsi.bund.de/ContentBSI/Publikationen/TechnischeRichtlinien/tr03125/index_htm.html [Online], accessed on December 2, 2010.

(4) Hühnlein, Detlef; Korte, Ulrike; Langer, Lucie; Wiesmaier, Alexander: A Comprehensive Reference Architecture for Trustworthy Long-Term Archiving of Sensitive Data. 3rd International Conference on New Technologies, Mobility and Security (NTMS). IEEE, 2009.

Dr. Lucie Langer
former researcher at the Cryptography and Computer Algebra Group at Technische Universität Darmstadt;
langer@cdc.informatik.tu-darmstadt.de

Dr. Alex Wiesmaier
senior researcher at the Center for Advanced Security Research Darmstadt (CASED);
wiesmaier@cased.de

Prof. Dr. Johannes Buchmann
head of the Cryptography and Computer Algebra Group at Technische Universität Darmstadt and director of CASED;
buchmann@cased.de