enisa
European Network and Information Security Agency

PRACTICAL GUIDE / ROADMAP FOR A SUITABLE CHANNEL FOR SECURE COMMUNICATION

Concise version

Secure Communication with the CERTs & other stakeholders

Report, December 2011

About ENISA

The European Network and Information Security Agency (ENISA) is a centre of network and information security expertise for the EU, its member states, the private sector and Europe's citizens. ENISA works with these groups to develop advice and recommendations on good practice in information security. It assists EU member states in implementing relevant EU legislation and works to improve the resilience of Europe's critical information infrastructure and networks. ENISA seeks to enhance existing expertise in EU member states by supporting the development of cross-border communities committed to improving network and information security throughout the EU. More information about ENISA and its work can be found at www.enisa.europa.eu.

Contact details

For contacting ENISA or for general enquiries on CERT related activities please use the following details:

- E-mail: cert-relations@enisa.europa.eu
- Internet: http://www.enisa.europa.eu

Contents

1 Executive Summary

This deliverable aims to give an overview of the work that was done in WPK 1.3 of ENISA's Work Programme[1] 2011. The goal of this work was to identify ways to improve communication with the CERTs and other stakeholders (institutions in the Member States, European Commission, etc.), especially when it comes to sharing information in a secure way. Secure in this respect means transportation of information and assuring some combination of confidentiality, integrity and authenticity of the data. ENISA wanted to identify the most suitable security technology and the channel to start with and to analyse a future secure communications platform, providing additional secure communication channels.

Both a stocktaking of existing solutions, developments and research in that area and an analysis of the requirements were performed in order to offer guidance on a suitable channel in this respect.

The stocktaking and the analysis have been used as inputs to preselect the technologies, solutions and products which are suitable, and to define the assessment criteria to select the suitable channels and security technologies. The assessment criteria applied to the evaluation has been grouped into four categories:

- Criteria regarding the suitable communication channel.
- Criteria regarding the security requirements.
- Criteria regarding CERT and stakeholders requirements.
- Criteria regarding CERT and stakeholders preferences.

[1] *http://www.enisa.europa.eu/about-enisa/activities/programmes-reports/work-programme-2011*

2 Introduction

2.1 Scope

In its Work Programme[2] for 2011 (WP2011) ENISA included an activity related to reinforcing CERTs in the Member States. One of the tasks defined in this work package was an analysis concerning ways to improve communication with the CERTs and other stakeholders (institutions in the Member States, European Commission, etc.), especially when it comes to sharing information, for example about incidents, in a secure way.

"Secure" in this context means information transfer ensuring some combination of confidentiality, integrity and authenticity of the data, possibly with non-repudiation.

The work, briefly described in this concise report has been extracted from a full detailed report 'Proposal for secure communication channel(s) and roadmap' which was developed for the CERT-EU pre-configuration team for future exploitation, together with the reports on the stocktaking and the analysis of the requirements of the stakeholders.

INTECO was commissioned by ENISA to undertake this study.

The aim of this project is to analyse the requirements of a secure channel for secure communication within the CERTs community and between them and other stakeholders, and to develop a practical guide and a roadmap for the implementation of the solution that best fits the requirements of this community.

2.2 Objectives

The main objective of the project "Secure Communications with the CERTs and other Stakeholders", which as mentioned above is one of the ENISA activities related to reinforcing communications between CERTs in the Member States, is the preparation work for a report on secure communication channel(s) with the CERTs and other stakeholders and a roadmap for implementation and future development.

The detailed objectives for this project were:

- To perform an assessment and solution selection: the different criteria for evaluating the possible solutions are defined by considering the security constraints, and the CERT and stakeholder requirements and preferences obtained during this project.
- To provide a description of the selected solution, in accordance with the identified requirements.
- To draft an implementation guide for the solution.
- To provide a solution implementation roadmap.
- To shed a light on possible future developments, detailing possible future initiatives and evolution as, for instance, the addition of new channels.

[2] *http://www.enisa.europa.eu/about-enisa/activities/programmes-reports/work-programme-2011*

This concise report aims at providing an outline of the results of this project.

3 Methodology

The work in this project consisted of three parts:

1) A stocktaking of existing solutions, developments and research in the area of interest;
2) An analysis of the requirements; and finally
3) The preparation of a practical guide and roadmap.

Both the stocktaking and the analysis activities had a similar approach and resulted both in a report which will be sent to the CERT-EU preconfiguration team for further exploitation together with the practical guide and roadmap report.

During the execution of both the stocktaking and the analysis part, CERT members, stakeholders and a number of experts in this field have been asked to comment on tools and methods used to secure communications in CERT community, with the purpose of having an in-depth analysis of the pros and cons of the existing situation and also collecting information and requirements for the optimal future solution.

The execution of these tasks has combined different kinds of methods with the purpose of achieving the project objectives in a sequential way and has aimed to identify as many synergies as possible between both parts. Three main methods were used:

1) Desktop research aimed to achieve a complete vision of the state of the art in secure communications solutions.
2) Expert Interviews (think tank, expert list defined in collaboration between InTeCo and ENISA).
3) A survey of requirements amongst CERTs/CSIRTs, stakeholders and experts, belonging to the European framework defined by ENISA.

4 Stocktaking of existing solutions, developments and research

The stocktaking report represents the results obtained from the different research activities performed (desktop research, interviews, interaction and surveys) with CERTs and other stakeholders and experts in the area of secure communications.

When security in communications is required, it is possible to take two different approaches to provide the security guarantees:

- Securing the data prior to being exchanged through an unsecure communications channel. In this approach, cryptographic technologies have been analysed: symmetric cryptography, asymmetric cryptography and hybrid cryptosystems (like PGP/GPG and PKI).
- Securing the communication channel as a whole, so any data being exchanged through that channel is secure. Technologies that secure the channel are SSH, SSL/TLS and VPNs.

Information regarding the current state of secure communications in the CERTs and stakeholders environment has been gathered during the data collection process, and this information is also presented in this report.

To align the research with the scope of this project, the application of the different technologies considered to the channels used in communications with CERTs and other stakeholders has been analysed. Channels considered are: email, instant messaging, file exchange / storage, VoIP, IRC and web.

The research and analysis activities carried in preparation of this report show that the most complete and widespread technologies are hybrid cryptosystems. This involves the integration of symmetric cryptography, asymmetric cryptography and hash algorithms in a unique communications technology. In this context, PGP/GPG is commonly used in email (and less used in other channels), while SSL/TLS is used in most of the channels analysed but barely in email in order to ensure the confidentiality of the communications. Both technologies are implemented by many existing solutions in the market.

The full stocktaking report will be provided to the CERT-EU pre-configuration team.

5 Analysis of the requirements

This analysis report is dedicated to the presentation and analysis of the results indicating which requirements were selected by participants as important or necessary. Different categories of requirements were analysed. Below are listed the requirements used in this analysis taking into consideration the inputs and feedback obtained from the qualitative and quantitative research. The detailed report will be provided to the CERT-EU pre-configuration team.

5.1 Security requirements

Security must be an integral part of any mechanism for exchanging information between CERTs and other stakeholders, since we are analyzing secure communications due to the sensitive nature or classification level of some information being transmitted.

- **Confidentiality**: a message is confidential when it can only be understood by the person or system authorized.
- **Integrity**: this is the quality by which a message or document can't be modified without the change being detected.
- **Authenticity**: means that a message or a document belongs to the person who claims it. Applied to the verification of the identity of a user, authentication occurs when the user can provide any evidence to verify that indeed s/he is who claims to be.
- **Non-repudiation**: in information security, non-repudiation implies that none of the participants of an information exchange can deny having sent or received a message.
- **Auditability**: is the quality by which a system can be examined or evaluated, in order to verify that it works how it is said that works. Auditability is also related to the ability of a system of having evidence of all operations made within that system, for example with access and operations traceability.
- **Restricted access**: means that the access to a system is not free or public; to achieve this usually is necessary to implement some mechanism to verify that the user accessing the system is an authorized user.

5.2 Interoperability requirements

Interoperability requirements refer to the ability of a system to work or integrate easily with other tools or standards.

- **Compatibility with information exchange standards/formats**: is the quality of a system to operate with established information exchange formats like, for example, IODEF.
- **Compatibility with existing tools**: refers to the ability of a system to integrate with other existing tools being already used such as, for example, incident management tools, CRMs, etc.
- **Integral communication solution**: is the quality by which a system or solution implements more than one communication channel.

5.3 Design requirements

Design requirements refer to the architectural characteristics of the solution.

- **Open source**: means that the source code of the solution is freely distributed. If a solution is open source, it implies that it can be audited.
- **Multiplatform**: is the ability of a solution to be run on multiple computer platforms and/or operating systems.

5.4 Performance requirements

Performance refers to the throughput performed by a system in relation to the time and resources used.

- **Performance**: in the scope of secure communication channels, information volume to transmit in a secure way per second (throughput).
- **Scalability**: growth capability, in terms of performance, in case of an increase in needs (new channels, more information volume...).

5.5 Functional requirements

Functional requirements are those characteristics or operations that should be implemented by a solution for secure information exchange in the CERTs environment.

- **Usability**: refers to the ease of use of a solution. To be usable, a computer software user interface should be intuitive and easy to learn.
- **Ease of deployment**: is related to the difficulty of installing a tool or technology in available infrastructures. It includes among others ease of installation, hardware requirements, etc.
- **Fault tolerance**: is the ability of a system to recover or continue working in the event of failure of some of its components.
- **Granularity**: refers to the possibility of specifying who has access to the information stored or being processed by a solution. It is usually related to access, users, roles and groups management.

5.6 Other requirements

In this section are listed those identified requirements that do not fit in any of the previous categories.

- **Trusted administrator**: means that the third party administrator or owner who is the provider of a solution must be trusted by all of the users. In other case, the users are not going to store or transmit sensitive information using a solution provided by a third party they do not rely on.
- **Not dependant on individuals**: this requirement refers to the capacity of a solution to be administered by an organization and not individuals. For example, the solution should keep working if the administrator or any other staff member leaves the company, and the channels used should not be established on personal basis.

- **Multiple manufacturers**: this requirement considers the possibility of similar solutions being provided by different providers. This could promote the competitiveness and overall quality of the solutions.
- **Commercial support**: refers to the solution having a manufacturer involved in its maintenance (although the solution itself could be open source).
- **Cost**: the cost of acquiring and implementing the solution.

6 Secure communications practical guide and roadmap

Based on the two reports 'Stocktaking of existing solutions, developments and research' and 'Analysis of requirements', a proposal was outlined for the implementation of a secure communication channel. A related roadmap to implement this channel was proposed too.

This practical guide and a detailed roadmap will be provided to the CERT-EU pre-configuration team together with the above reports for further exploitation.

The practical guide is both a user's guide for end users of secure communications and an implementation guide for ENISA to foster and support some of the infrastructure required by the secure communications platform required by CERTs and stakeholders.

An overview of the related roadmap is given below.

- **Project definition**: This will be the initial stage of the project, prior to the start of fostering activities and platform analysis, to review, approve and gain the commitment of the workgroup with the key project foundation. Several workgroup meetings would be held, where the members will have to agree on the following topics:
    - Convenience and viability of the implementation of a secure communications platform.
    - Existing tools and technologies analysis. Review of present project deliverables and proposal for secure communications platform
- **Platform development**: This task refers to the implementation of a common secure communications platform. Depending on the chosen implementation model and the resources assigned to the project, the duration of the tasks may vary. It includes the following activities:
    - **Requirements analysis**: in this phase the platform requirements must be specified. Possible topics would be the channels to implement, identity management, etc. The input for this activity would be this deliverable, but deep analysis should be carried out to complete and detail it.
    - **Design**: once the requirements are defined, how they will be met is determined in the design phase. Topics to deal with in this phase would be the architecture of the solution, interaction between components, etc. Again, this deliverable would be an input for this activity, but more comprehensive detail will be performed before going into implementation.
    - **Implementation**. This is the coding phase, following the requirements and design specifications.

- **Testing**. Testing phase, to assess the quality and security of the solution. This phase also includes the resolution of problems detected in the testing process.
- **Platform publishing**. When the testing phase has finished, the platform software would be distributed among the participants (published in a web portal, sent by email,...).
- **Maintenance of the platform**. This phase would not have end date, since the platform will require at least a minimal maintenance while it is in use.

- **Fostering**: Within the task "Fostering" we can have any number of subtasks and milestones that would mainly consist of providing publications and attending events:
  - Attend relevant events/conferences organized by CERTs and/or stakeholders to promote the use of secure communications.
  - Activities at events could include presentations, publications delivery (see below), workgroup meetings (see below) or key signing parties.
  - Some examples of events to attend are the TERENA's TF-CSIRTs meetings organised by ENISA, FIRST meetings, APWG events, e-Crime congresses, MAAWG events or other European institutions events.
  - Releasing publications about secure communications, procedures and best practices for CERTs and Stakeholders. These publications could be delivered in events, as well as published through ENISA's portal.
  - Promoting the platform implementation and utilization.
  - Workgroup: creation of a workgroup with the participation of CERTs and stakeholders, to monitor and support the implementation and adoption secure communication.
  - The workgroup could hold meetings at events already scheduled (e.g. TF-CSIRT).
  - ENISA could support the use secure communication by using it in their own communications and media (signing/encrypting emails, web pages, documents, etc.) or for online registration in events organised by ENISA.
- **The web of trust. Key management and directory creation**, with the identities and certificates of CERTs and Stakeholders. This would take place simultaneously with other "Fostering" activities. The workgroup could provide support on these activities as well.

- **Key management infrastructure**: This phase will follow the necessary steps to create the key management infrastructure. The size of the platform will directly depend on the focus adopted for the key management, having two options:
  - Creation of a single root, housing the public keys of all CERTs and stakeholders wishing to become part of this community.
  - Creation of a main root and several secondary platforms, being part of the main root the CERTs and also the European level stakeholders (e.g. Europol), and the rest of platforms, being one per country, containing the public keys of the various CERTs and stakeholders in that country. This seems to be the most recommendable option.
- **Key management platform publishing**: when the initially defined group of members of a particular the key platform is complete, the key platform access point can be published. The web directory with the identities could also be published.
- **Key management platform maintenance** & **monitoring**: to develop and maintain the PKI.

- **Monitoring of the adoption level of secure communication**, to check the implementation level in CERTs and stakeholders' environment, and the different promotion activities held during the implantation execution. The workgroup could provide support on these activities too.

7 Conclusions

One of the results of the stocktaking of existing solutions, development and research, is that CERTs use a variety of secure communications channels and that most complete and widespread technologies are hybrid cryptosystems.

Concerning the requirements, there are several requirements to be considered for secure communication channels, from security requirements to the interoperability ones, from design to performance or functional requirements.

A clear conclusion from the stocktaking and the analysis of the requirements is that CERTs currently use within the CERT community a PKI based secure communication solution. It is also a clear requirement of secure communication for most CERTs. A widely used example in the CERT community is PGP.

An overview of the proposed secure communications practical guide as well as of the related road map for implementation and future development of secure communication channels with the CERTs and other stakeholders was provided to the CERT-EU pre-configuration team.

P.O. Box 1309, 71001 Heraklion, Greece
www.enisa.europa.eu