Indispensable baseline security requirements for the procurement of secure ICT products and services

1 Introduction

The procurement of key ICT products or outsourced managed services may result in intentional or unintentional security risks and incidents. In 2012 the EC drew up detailed guidelines[1] on how to make best use of ICT standards in tender specifications in the context of Action 23 of the Digital Agenda of Europe and in 2013 issued a Communication on Standardisation and Public Procurement[2] . Use of standards promotes a level playing-field, allowing a broader range of participation, including SMEs, and avoids "lock-in" to specific brands with proprietary features. However, due to the evolution of technology in ICT and the lack of expertise to decide which standards are relevant and appropriate for the particular ICT needs, it is not always the case that ICT procurements are standards-based.

Therefore, it is important to help procurers overcome these difficulties through common and sufficiently generic minimum indispensable requirements that will cover the whole lifecycle of the procured product or service and will eventually contribute to an appropriate (and desired) minimum level of security and resilience. In this context, ENISA set up an Expert Group composed of experts nominated from Member States to identify existing best practises and requirements and to use them to identify a set of indispensable baseline security requirements. This collaborative approach will support all Digital Single Market stakeholders to develop a more unified, integrated and cost-effective approach for standards-based procurement of secure ICT products, and helps providers in specifically dealing with security risks involved in the procurement and outsourcing processes.

1.1 Purpose

This document can be of use to suppliers and procurement officers when planning, offering and purchasing ICT products, systems and services. It is meant as a practical, technologically neutral document with clear, simple and sector-agnostic minimum necessary indispensable requirements for secure ICT products and services. Any ICT product or service that fails to be compliant with one or more of the minimum security requirements should be considered as insecure and therefore it shall not be purchased or put in operation on the Digital Single Market (DSM). It focusses on a few indispensable conditions, commonly agreed among experts and based on standards and best practices, but does not claim to cover completely and sufficiently all possible security requirements. It is not intended to substitute existing security certifications schemes and standards: instead it is a complementary security baseline.

[1] http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=2326
[2] http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=2327

1.2 Approach

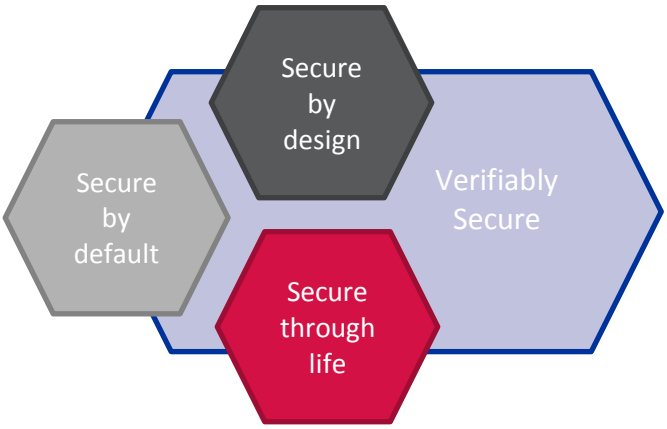

Figure 1: Four principles for supply and procurement

Figure 1 above depicts the four principles that were stated by the Expert Group as a basis for the development of the indispensable requirements. Components of the system, the services that they and the system use, and the services the system provides shall be secure:

- By design – the product, or service, has been conceived, designed and implemented to ensure the key security properties are maintained: availability, confidentiality, integrity and accountability.
- By default – the product, or service, is supplied with the confirmed capability to support these security properties at installation.
- Throughout their lifecycle – security should be maintained from initial deployment through maintenance to decommissioning.
- And that each of the above principles should be verifiable.

The indispensable baseline security requirements are expressed as a limited collection of principles written, as far as possible, in non-specialist terms – a set of "Commandments" listed in Section 2. In addition, Section 3 provides explanations and examples than can be used for compliance checks.

1.3 Obligations for the Customer (Procurer)

The security requirements for the specific ICT system will have wider, or different, scope than those stated in this baseline and will be identified by a risk-assessment that takes account of the desired system objectives and the prevailing security landscape. The baseline may be sufficient but users of this guide must ensure that security requirements beyond the baseline are fulfilled effectively by appropriate measures.

2 Overview of Indispensable Baseline Security Requirements

Note: All the requirements presented below apply also to the supplier's subcontractors or its third party service providers.

Security by Design	**The provider shall design and pre-configure the delivered product such that functionalities are based on well-established security practices and are reduced to the strict minimum required for system operations.**
Least Privilege	**The provider shall design and pre-configure the product according to the least privilege principle, whereby administrative rights are only used when absolutely necessary, sessions are technically separated and all accounts will be manageable.**
Strong Authentication	**The product shall provide and support strong authentication mechanisms for all accounts. If authentication is unsuccessful the product shall not allow any user specific activities to be performed.**
Asset Protection	**The product shall provide adequate level of protection for critical information assets during storage and transmission.**
Supply Chain Security	**The provider shall give means to ensure that the product is genuine, cannot be tainted during operation, and its integrity are warranted throughout the product's lifecycle.**
Documentation Transparency	**The provider shall offer comprehensive and understandable documentation about the overall design of the product, describing its architecture, functionalities and protocols, their realisation in hardware or software components, the interfaces and interactions of components with each other and with internal and external services, in order to be able to implement and use the product in the most secure way possible.**

Quality Management	**The provider shall be able to provide evidence that a managed security by design approach has been adopted, including documented secure software development, quality management and information security management processes.**
Service Continuity	**The provider shall guarantee support throughout the agreed lifetime of the product such that the system can work as agreed and is secure.**
EU Jurisdiction	**The provider shall accept that all contracts refer to EU Member State law and only EU Member State law and place of jurisdiction in an EU Member State country and only an EU Member State country, including those with subcontractors.**
Data Usage Restriction	**The provider shall explicitly declare, justify and document, context and purpose wise, all data collection and processing activities that take or may take place, including relevant legal obligations stipulating them.**

3 Guidance on using the requirements

This Section provides more detailed explanation of requirements that the supplier shall address in complying with the baseline requirements.

3.1 Security by Design

The provider shall design and pre-configure the delivered product such that functionalities are based on well-established security practices and are reduced to the strict minimum required for system operations.

- Functionalities that are not needed shall not be installed.
- Functionalities that are installed shall have no undocumented capabilities, especially not those that run against the security and privacy interests of the operator (free from malware, spyware, hidden functionalities, un-documented backdoors or any other unapproved or unwanted functionalities such as non-authorised data forwarding).
- Logging and auditing functions shall be included and supported by design. They shall be based on open interoperable standards and best practices in order to work properly with Security Information & Event Management (SIEM) and logging and monitoring systems.
- The system shall log user activities as well as security relevant events and errors in a format that can be evaluated and analysed during operations or afterwards. The log files shall be protected against tampering.
- All systems shall provide a widely acceptable standard system time and possibility to sync it with an external time source in order to achieve exactness of system time to the second.
- The supplier shall not use technologies, protocols and functionalities that are outdated or already recognised as insecure (e.g. SSL 3.0, MD5, or RC4, among others)
- The complete system with all its components, i.e. including extensions and enhancements, must be ready for mitigating known vulnerabilities.

3.2 Least Privilege

The provider shall design and pre-configure the product according to the least privilege principle, whereby administrative rights are only used when absolutely necessary, sessions are technically separated and all accounts will be manageable.

- An administrator shall be able to manage all accounts (incl. technical and service accounts) without support from the provider.
- Every service and every user shall have by default only the minimal rights that are required for specific activities.
- Every user shall obtain its own user account.
- Passwords shall be changeable in all cases by the operator.

- The password complexity must be configurable by the administrator:
  - minimal password length;
  - maximum password length (system must support at least up to 128 characters);
  - minimum number of specific characters or character groups, e.g. small and capital letters, numbers, special characters (incl. space), etc.;
  - minimum and maximum usage period;
  - prevention of re-use of previous passwords; and
  - maximum number of password changes per time (e.g. per day).

3.3 Strong Authentication

The product shall provide and support strong authentication mechanisms for all accounts. If authentication is unsuccessful the product shall not allow any user specific activities to be performed.

- Applications shall have the capability to enforce rules or policies for identification and authorisation of users that execute them.
- Access to data shall only be given after successful authentication and authorisation. Without successful authentication and authorisation, the system shall not allow any activities.
- Service accounts shall not be usable for interactive logon.

3.4 Asset Protection

The product shall provide adequate level of protection for critical information assets during storage and transmission.

- Physical assets are the products that the provider supplies to the operator to be installed, including equipment of any kind, documentation, and premises.
- Logical assets are the information generated by applications, stored, and communicated between components of the system.
- Physical and logical assets shall be verifiably protected during design, manufacture, delivery, operation, and decommissioning.
- No cryptographic means shall be used if there are indications that they have been vulnerable to cryptanalysis.
- Sensitive data (e.g. credentials) may be stored in the system respectively transmitted only in encrypted form
- Only established and well-known encryption algorithms may be used and encryption key lengths, which are considered as safe according to the state-of-art. Proprietary encryption algorithms are not allowed.

- The implementation must be done based on well-established encryption libraries to avoid implementation weaknesses.
- The key generation must create secure keys and keys must be stored securely.

3.5 Supply Chain Security

The provider shall give means to ensure that the product is genuine, cannot be tainted during operation, and its integrity are warranted throughout the product's lifecycle.

- The authenticity checking method(s) of the product shall be capable of tracing back software and/or hardware components to their genuine sources.
- The authenticity checking method of the product shall protect the properly authorized configuration information assets of the system.
- The integrity checking method shall be capable of verifying the correctness of all compatibility and dependability requirements in the product.
- Ongoing authenticity and integrity checks during operations shall detect and indicate any unauthorized change in the configuration of the system.

3.6 Documentation Transparency

The provider shall offer comprehensive and understandable documentation about the overall design of the product, describing its architecture, functionalities and protocols, their realisation in hardware or software components, the interfaces and interactions of components with each other and with internal and external services, in order to be able to implement and use the product in the most secure way possible.

- The documentation shall be updated securely without the need for a permanent reference to external servers.
- The documentation shall be updated when there are major changes to design or functionality.
- Users shall be made aware of changes to documentation and encouraged to switch to the new documentation set.

3.7 Quality Management

The provider shall be able to provide evidence that a managed security by design approach has been adopted, including documented secure software development, quality management and information security management processes.

- The provider should possess a current valid security certification in the relevant area or something equivalent (e.g. development, production), such as ISO27001 or corresponding).
- At least, a rationale of fulfilment of requirements addressed by such security or quality assurance certifications should be available
- The provider shall be able to provide the relevant information security directives which are applicable to its product/service.

3.8 Service Continuity

The provider shall guarantee support throughout the agreed lifetime of the product such that the system can work as agreed and is secure.

- The provider shall guarantee:
  - A minimum lifecycle during which support is assured.
  - An ongoing research for potential vulnerabilities (e.g. a responsible disclosure program).
  - If critical vulnerabilities (according to their CVE rating) get known, the provider is obliged to check in a timely manner and at his own expense, whether his product is affected by the weakness and to inform the operator of the result.
- Timely provisioning of security patches or other appropriate risk mitigation measures, when new vulnerabilities get known. As a first remediation step the provider should at least respond with a remediation plan at the latest within seven (7) working days. The plan shall indicate the timeframe for resolving the vulnerability.

3.9 EU Jurisdiction

The provider shall accept that all contracts refer to EU Member State law and only EU Member State law and place of jurisdiction in an EU Member State country and only an EU Member State country, including those with subcontractors.

- The provider must inform the operator about non-EU laws that it is obliged to obey.
- The provider shall inform the operator about all countries' laws that apply to the operator by using its product and services.

3.10 Data Usage Restriction

The provider shall explicitly declare, justify and document, context and purpose wise, all data collection and processing activities that take or may take place, including relevant legal obligations stipulating them.

- The provider shall inform the operator about non-EU laws that must be obeyed concerning data collection or forwarding.
- The provider and the operator shall agree on the use of the Traffic Light Protocol (TLP) when sharing security relevant information between operator, provider, supplier(s), other operators, end users and the general public.

4 Conclusions

This document introduced the need for a set of indispensable baseline security requirements that will be used by procurers and suppliers of ICT systems and services. The approach to developing such requirements was outlined along to the requirements themselves followed by clarifying examples of detailed issues that must be addressed. Envisioned next steps include consultation with European Cyber Security Organisation (ECSO) community as the established representative of private sector from all sectors, to initiate a broader discussion, structured feedback and improvements in order to find consensus on the applicability of this document. Subject to advice from the community, future work could include a mapping of the baseline requirements to a catalogue of relevant standards, and further detail on the verification that ICT products are secure: by design, by default, and throughout their life.

Contact

For queries in relation to this paper, please use isdp@enisa.europa.eu

Acknowledgements

ENISA would like to thank the following members of the Expert Group for their active engagement and support throughout this activity: Mr. Wolfgang Schwabl - A1 Telekom Austria AG (AT), Mr. Thomas Stubbings - TSMC (AT), Mr. Aurélien Leteinturier - ANSSI (FR), Mr. Tobias Mikolasch - BSI (DE), Mr. Martin Konecny - NBU (CZ), Ms. Gema Carbonell - CCN (ES), Mr. Rob Huisman - NINCSA (NL) and Ms. Heidi Kivekäs - FICORA (FI).