AutoPASS –SFAP Security framework

Version log

Version	Initials	Date	Comments/amendments
0.9	JEM	12.06.17	Preliminary RFP sent to Bidders
1.0	JEM	05.07.17	RFP sent to Bidders
1.1	CS	15.09.17	Correction of minor errors and clarification of how to complete the document
1.2	TLI	08.01.2020	
2.0	HL	04.02.2020	Released for announcement

1.1 Introduction

This Annex contains the Security Policy for AutoPASS draft, and is to be completed by the bidder and added to Appendix2 as a separate Annex.

Instruction to Bidder: *Text in (blue) < italic > contains instructions to Bidder as to how this document shall be filled out and completed by the Bidder. The Bidder's response shall be made in the colour blue. Any mark-ups beyond the requested response shall be made in Appendix 8.*

1.2 Security objectives

The SFAP security policy shall be guided by the security objectives listed below. They express a general guideline and shall, in the case of a conflict with any of the detailed requirements in Appendix 1, have a higher priority. They can also serve as a management summary of the approach to security in SFAP. The security objectives are numbered as SO-n.

<[SO-1] Any SFAP toll data exchanged between a TC and a TSP shall fall under the SFAP security rules

The SFAP security rules apply only to the toll data relevant for the SFAP services.

[SO-2] SFAP toll data shall be correct, complete, traceable and protected

- *Correct SFAP toll data fully and accurately records all required road usage parameters according to the rules of the SFAP toll scheme.*

  This statement also covers the transmission of data between actors and thereby delivers data integrity in communication.

- *Complete SFAP toll data means that no toll data is deliberately or otherwise lost according to the rules of the SFAP toll scheme.*

  As a complement to the correctness requirement, toll data must also be complete. That means that no data that shall be reported can be suppressed. This statement emphasises the need to secure not only correct recording, but also correct reporting and thereby ensures data availability.

- *Traceable SFAP toll data can be traced back to its originator/owner in a manner that its veracity can be contested and proved with enough confidence to be able to stand as evidence in a dispute.*

  As data is refined through its process chain, passing from one actor to another, the responsibility and ownership of data must be clear at each step. In particular, if errors or falsifications are added in one part of the chain, while the other parts are correct and in compliance with system requirements, it shall still be clear which actor is accountable.

- *Protected SFAP toll data can only be accessed by authorised parties.*

  The various SFAP systems shall for all parts of the SFAP toll data clearly define which actors under which conditions can access it. The upholding of these definitions shall be supported by cryptographic, administrative and/or other procedures. This statement delivers data confidentiality.

NOTE: SO-2 thus covers the Confidentiality-Integrity-Availability (CIA) triad

[SO-3] Risk and efficiency should be considered when implementing security in SFAP

As large funds will be transferred between the individual actors in the SFAP toll scheme it is a top priority that it delivers a high level of security and reliability. It is very important that the toll due for the usage of an infrastructure can be imposed on the correct service user which used this infrastructure.

It will never be possible to achieve perfect security and reliability in any operational system. Rather, the question is how reliable and secure a system has to be to fulfil its needs for the involved actors. At a certain point, the marginal costs that must be incurred in order to increase security and reliability one more step will represent a disproportionate effort where the costs will exceed the additional benefits.

The evaluation of risk and efficiency shall be made when implementing the requirements and security measures based upon the threat analysis from the EFC security framework CEN TS 16439.

Costs and benefits shall in this context refer to both the economic resources of all actors and to the time and effort needed from the service user to be compliant with the system.

[SO-4] The SFAP security requirements shall be limited to supporting interoperability between the involved actors

SFAP is a compound of many separate toll domains that differ in many ways, for example in technical solutions, legal requirements and operational procedures.

The different charging scenarios shall be respected, possibly leading to specific security requirements for the different types of toll domains. The common security requirements resulting from this policy shall therefore be limited to the common aspects of the whole of SFAP.

- *Security requirements shall be applicable to different charging scenarios: barriers vs. free-flow*
- *different technical solutions:, DSRC vs. autonomous systems*
- *different legal requirements: fee vs. tax*
- *different operational procedures: mandatory vs. non-mandatory OBU*

This limitation in scope represents a pragmatic recognition of the history of the currently participating toll domains and the difficulty of fitting them into a common interoperable framework as well as to expand the SFAP service to new toll domains.>

1.3 Policy statements

The security policy contains policy statements on how it is intended to protect information in SFAP. Each statement requires more detailed procedures and practices to be implemented which in turn will contribute to the overall reduction in risk as a whole. The security policy is a way of assuring the confidentiality, integrity and availability of assets in the SFAP and its information and communication architecture and infrastructure for the benefit of the service users and the TC`s and SP`s participating in SFAP.

1.3.1 General policy statements

[PS-1] <The objective of the information security is to:

- *ensure confidentiality, integrity and availability of all information in the EFC service operation and management;*
- *prevent and limit the consequences of unwanted or unexpected information security events;*
- *build the required trust and confidence between the involved actors.*

[PS-2] SFAP will use international and European security standards and European and national legislation for personal data integrity.

The standards

- *ISO/IEC 27001:2015 Information technology -- Security techniques -- Information security management systems -- Requirements"[1]*
- *"ISO/IEC 27002:2015 Information technology – Security techniques – Code of practice for information security management"[2] and*
- *EFC Security Framework[3]*

shall adhere to in the SFAP information security or equivalent standards, guidelines or specifications, like the "IT-Grundschutz Catalogues" of the German Federal Office for Information Security.[4]

[PS-3] The SFAP information security shall provide the involved parties with the means (specifications, procedures, etc.) to fulfil legal, regulatory and contractual requirements regarding information security, data protection and privacy.

[PS-4] Sensitive personal data shall be protected by reasonable security safeguards against the risks of loss or unauthorised access, destruction, use, modification or disclosure of data.

The rules of the EU Directive 2006/24/EC on data retention shall be observed, and the solution shall be prepared for any implementation in Norway of the directive.>

1.3.2 Organisational policy statements

[PS-5] <SFAP information security shall be governed, developed and managed by the interoperability management to be established by <NPRA and RBPS> and reviewed by the actors in SFAP.

The interoperability management shall develop, coordinate and maintain and constantly improve the SFAP information security.

The actors in SFAP shall support the implementation of the SFAP information security and review all actions taken by the SFAP actors.

The actors in SFAP shall provide the resources required for these tasks.

[PS-6] The SFAP Interoperability Management shall develop and maintain the Security Policy.

WP5 will define the rules for the work of the Interoperability Management.

[PS-7] The interoperability management shall develop and maintain the selected SFAP security requirements. All security requirements shall be chosen from the EFC security framework based on the return on experience of the SFAP partners in EETS, and a continued risk and vulnerability evaluation including a simplified risk analysis.

---

[1] Covers all types of organisations (e.g. commercial enterprises, government agencies, not-for-profit organisations) and specifies the requirements for establishing, implementing, operating, monitoring, reviewing, maintaining and improving a documented information security management system within the context of the organisation's overall business risks. It specifies requirements for the implementation of security controls customised to the needs of individual organisations or parts thereof.

[2] Establishes guidelines and general principles for initiating, implementing, maintaining and improving information security management in an organisation.

[3] Describes a set of requirements and security measures for stakeholders to implement and operate their part of an EFC system as required for a trustworthy environment according to its basic information security policy. In general the overall scope is an information security framework for all organisational and technical entities and in detail for the interfaces between them.

[4] Since a majority of the requirements and security measures in the draft EFC Security Framework are optional, adhering to the standard still requires selecting the appropriate ones. This should be done in the SFAP security requirements document and in the SFAP security specification respectively.

The SFAP information, assets, interfaces and processes shall be assessed and grouped to indicate the need, priorities and expected degree of protection.

[PS-8] The interoperability management shall develop and maintain the SFAP security specification. All security measures shall be derived from the identified security requirements. The choice of security measures shall be based on the required level of protection.

The chosen security measures shall be capable of preventing, detecting, tracking and handling unwanted information security incidents.

[PS-9] The interoperability management shall develop and maintain the SFAP security test procedures to enable the testing of SFAP actors' assets, interfaces and processes. The SFAP security test procedures shall be able to prove the compliance to all security measures and security requirements.

[PS-10] The SFAP information security shall be subject to regular reviews with planned intervals or when significant changes related to information security occurs.

Regular risk evaluations shall be carried out as a revision of the SFAP security measures and operative practice. In addition, risk evaluations shall be carried out when there are significant changes to the threat situation or vulnerabilities have been detected.

[PS-11] The default solution to establish initial trust between the SFAP operators (Toll Chargers and SFAP Providers) shall be a peer-to-peer trust model but a mixed model also allowing for hierarchical trust models shall be supported as well.

[PS-12] Technical audits will be undertaken, as determined by the SFAP interoperability management. Any technical audit work must be carried out under the supervision of technically competent and authorised personnel.

Any auditing of operational systems shall be carefully planned to minimise disruption to the continuous operation of the system. All auditing work requires an approval from the management of involved system(s) before it starts.

Such audits may include penetration testing after the targeted SFAP actor or asset has been informed.

[PS-13] The auditing of live data shall be limited to read only checks. Any type of audit requiring a change of data shall be carried out on copies of the data, which shall be destroyed after it is no longer required.>

1.3.3 Asset and interface management policy statements

[PS-14] <There shall be a compliance check for all new assets, interfaces and processes introduced by existing or new SFAP actors based on the SFAP security test procedures.

[PS-15] The level of SFAP information security shall not be reduced by the introduction of new SFAP actors, services or products.

[PS-16] All SFAP assets shall be accounted for and have a nominated owner.

[PS-17] Any users of SFAP assets shall be granted access to the appropriate systems, their resources and their information only after this access was authorised by the owner of the asset.

Anyone granted access to SFAP assets shall follow the internal guidelines for secure use. These internal guidelines for secure use will be included as a set of measures in the SFAP security specification and shall be adopted by each SFAP actor.

[PS-18] Full traceability of processed information shall be guaranteed at all times.

[PS-19] The interoperability management shall maintain a process for suppliers and TSP to get their components and procedures qualified with regards to the SFAP security test

procedures specified by WP2. The process shall also apply to additions and modifications to the components and procedures.>

1.3.4 Incident management policy statements

[PS-20] <The SFAP information security shall limit the consequences of unwanted information security incidents.

[PS-21] Anyone using the SFAP assets shall report any unwanted information security incident or violation of the SFAP information security to the interoperability management.

The interoperability management shall initiate a security revision and/or other necessary internal inspections to accommodate a systematic improvement and learning process to minimise the risk of similar events and non-conformances.>

1.4 Information Security Management System

The requirements as in *Table 1* have been identified as of interest in the SFAP.

For each class of requirements, a table has been produced, where for each requirement the SFAP selection is expressed in terms of either **M** (Mandatory) or **R** (Recommended).

<

No	Requirement	SFAP selection (M/R)
RQ.ISMS.1	Establish, implement, operate, monitor, review, maintain and improve an Information Security Management System (ISMS) according to ISO/IEC 27001	M

Table 1. ISMS requirements

The following Table 2 shows the requirements related to the above interfaces.

No	Requirement	DSRC (M/R)	TC/TSP Interface (M/R)	Comm. Provider (M/R)
RQ.IF.02	Data exchange shall be done using transmission channels with reliable availability.	M	M	M
RQ.IF.10	Data exchange shall guarantee data confidentiality.	R	M	M
RQ.IF.11	Data exchange shall guarantee data integrity.	M	M	
RQ.IF.12	Data exchange shall guarantee the authenticity of the data originator.	M	M	R
RQ.IF.13	Data exchange shall guarantee non-repudiation with proof of origin.	M	M	R

No	Requirement	DSRC (M/R)	TC/TSP Interface (M/R)	Comm. Provider (M/R)
RQ.IF.14	Data exchange shall guarantee non-repudiation with proof of delivery.		M	R
RQ.IF.30	Data exchange shall allow the detection of resent messages (protection against replay attacks).	M	M	

Table 2 Interface requirements

The following Table 3 shows the requirements related to data storage.

No	Requirement	OBE	RSE
RQ.DS.01	Access to stored data shall only be granted after authorisation.	R	M
RQ.DS.02	Access to stored data shall only be granted via defined interfaces and defined procedures.	M	M
RQ.DS.03	Stored data shall have an independent backup of the data stored elsewhere.		
RQ.DS.05	Data storage shall guarantee data integrity.	M	M

Table 3 Data storage requirements

The following Table 4 shows the security requirements for Interoperability Management.

No	Requirement	SFAP selection (M/R)
RQ.IM.01	The Interoperability Management shall issue an EFC scheme security policy in collaboration with the involved stakeholders.	M
RQ.IM.02	The Interoperability Management shall have or define one or more auditing bodies supervising the security implementation of the TSP and TC involved in the interoperable EFC scheme.	M

Table 4. Interoperability management requirements

>

1.5 Yearly revision

There will be a yearly revision based on ISAE 3402-II for the TC and TSP solution.

(http://isae3402.com/ISAE3402_reports.html)