SECREDAS

Product **Se**curity for **Cr**oss Domain R**e**liable **D**ependable **A**utomated **S**ystems

Questionnaire on Safety Security Privacy Standards

SECREDAS has received funding from the Electronic Component Systems for European Leadership Joint Undertaking under grant agreement nr.783119. This Joint Undertaking receives support from the European Union's Horizon 2020 research and innovation programme and Austria, Belgium, Czech Republic, Germany, Finland, Hungary, Italy, The Netherlands, Poland, Romania, Sweden and Tunis

Executive Summary

For studying the state-of-the-art of Safety, Security and Privacy (S-S-P) standards, we designed this questionnaire for all participants of SECREDAS. The questionnaire aims to obtain an overview on the standards which interest the SECREDAS partners. It is combined with a planned general survey on standardization and serves as a single source of information for the first deliverable of WP10.

The survey intends to reveal the acceptance of existing (inter)national standards in both industry and academia, the application of standardized or proprietary S-S-P engineering methodologies, and the maturity of the available S-S-P technologies with respect to the standards. We also solicit feedbacks about your involvement in the related standardization activities with respect to (highly) automated systems, your preview on evolving standardization activities in the international standardization organizations, as well as the challenges and opportunities you see for influencing standardization, either in maintenance of existing standards or even proposing new work item proposals.

We will present the result of the survey to all SECREDAS participants in a WP10 deliverable and also in the 6-month consortium meeting, so that you could see a landscape of related standards. Any information from your reply which involves individual persons or organization will not be published without consent. Only aggregated and anonymized data will be presented in SECREDAS deliverables.

The survey should take about 15 minutes. Please kindly reply to us before **12 Nov 2018**. If you have any questions, please email us: Lijun.shan@internetoftrust.com and claire.loiseaux@internetoftrust.com. For returning your reply, please indicate your organization in the file title i.e. “Secredas Questionnaire on Standards - XXX”.

We really appreciate your input!

Table of Contents

Executive Summary **2**

1 About you and your organization ***4***

2 Overview of standards ***5***

2.1 Standards and standardization **5**

2.1.1 Cross-domain standards 6

2.1.2 Automotive 8

2.1.3 Rail 9

2.1.4 Health 10

2.2 Your expectation on future standards **11**

3 Your usage of standards in building products or services ***12***

3.1 Your products or services **12**

3.1.1 For technology developers 13

3.1.2 For technology integrators 14

3.1.3 For service providers 15

3.2 Your usage of methodologies, tools and models **16**

3.2.1 Safety Security Privacy engineering methodologies 16

3.2.2 Safety Security Privacy engineering tools 17

3.2.3 Safety Security Privacy models 18

4 Your usage of standards in assessment activities ***19***

5 Open questions ***20***

5.1 On reuse and patterns **20**

5.2 On quality assurance **20**

5.3 Other concerns or comments **21**

1 About you and your organization

Question	Answer [1]
Your name and title	
Name of your organization	
Domain of your organization (e.g. auto, health, rail, IT, etc.)	
Type of your organization (e.g. OEM/Tier 1/Tier2, service, research institute, plus[2] SME if applicable)	
Your main participation in SECREDAS (WPs or tasks)	
Your contribution to SECREDAS in terms of solutions, technology, products or services	
Type of your main clients	
Type of your main suppliers	
Type of your main research cooperators	
Geographic zone of your clients or your product deployment or your research cooperation (e.g. Europe, Asia, US, etc.)	
In which country/countries (or Europe) do you (intend to) qualify/certify your products or services	

[1] Please write "N/A" if not applicable.

[2] "plus" means you can give two answers addressing the "plus" topic as well.

2 Overview of standards

This section investigates your application of Safety Security Privacy (S-S-P) standards and your interest or participation in the development of standards. The standards listed below are from our state-of-the-art study. Please feel free to add any standards which interest you, including those under development.

2.1Standards and standardization

The following subsections are oriented to SECREDAS partners according to their domains: subsection 2.1.1 is for all partners; subsections 2.1.2 – 2.1.4 are devoted to partners which are active in automotive, rail and health domains, respectively. Please specify your answers in the corresponding columns of each subsection:

(1) **Develop or observe**: Do (or will) you participate in or observe the development of certain standards? Please specify *Participate* (please also indicate your role[3] and the relevant WG/TC/SC), *Will participate* or *Observe*, if applicable.
(2) **Apply standards in**: In which activity of your daily work do (or will) you apply certain standards? Please specify *Product/service development*, *Research project*, *Testing service*, *Assessment service*, *Consultancy service*, *Training*, or other activity, if applicable.
(3) **Evaluate conformance by**: In the case of applying some standards, how do you evaluate the conformance to the standards? Please specify *Self-evaluation*, *3rd party evaluation*, *Qualification* and/or *Certification*, if applicable.
(4) **Why apply**: What is your reason of applying certain standards? Please specify *Required by customers*, *Required by regulation*, *Guideline for performance*, *Assurance of quality of product/service*, or other, if applicable.
(5) **Why didn't apply**: What is the reason of not applying certain standards? Please specify *Irrelevant*, *Not mandatory*, *Too demanding*, *Too costly*, *No available tool*, *No benefit expected*, or other, if applicable.

[3] Please indicate your role:
- *A* = Active member (taking part in F2F meetings etc.) of a Work Group (WG)/Technical Committee (TC)/Sub Committee (SC)
- *M* = Member of a WG/TC/SC
- *C* = Convener, Leader, Chair of a WG/TC/SC

2.1.1 Cross-domain standards

	Standards		Develop or observe	Apply standards in	Evaluate conformance by	Why apply	Why didn't apply
Safety	IEC 61508	Functional safety					
	ISO 13849	Safety of machinery -- Safety-related parts of control systems					
	IEC 62061	Safety of machinery – E/E/PE control systems					
	Others, please specify						
Security	IEC 62443	Industrial network and system security					
	ISO 27000 family	Information security					
	ISO 15408	Common criteria					
	NIST 800	Computer security					
	Others, please specify						
Privacy	ISO 29100	Privacy framework					
	ISO 27550	Privacy engineering					
	Others, please specify						
Safety Security Privacy co-engineering	IEC TR 63069	Framework for functional safety and security					
	Others, please specify						
Dependa-bility	IEC 62853	Open systems dependability					
	IEC 62741	Demonstration of dependability requirements					
	Others, please specify						
Enterprise IT architecture	TOGAF	Architecture framework					
	IEC 62541	OPC unified architecture					
	Others, please specify						

Internet of Things	ISO/IEC 30141	Internet of things - Reference architecture					
	Others, please specify						
Others cross-domain standards, please specify							
E.g.	*Security*	*ISO 15408*	*Common criteria*	*Participate (A, ISCI)*	*Consultancy service*	*3rd party evaluation by licenced CC labs*	*Required by Customers, for certifying their products e.g. Secure Elements*	*N/A*

2.1.2 Automotive

	Standards		Develop or observe	Apply standards in	Evaluate conformance by	Why apply	Why didn't apply
Safety	ISO 26262	Road vehicles – Functional safety					
	ISO PAS 21488	Road vehicles – Safety of the intended functionality					
	ISO 26262 Ed2	Road vehicles – functional safety					
	ISO 20077	Extended vehicle (ExVe)					
	Others, please specify						
Security	SAE J3061	Cybersecurity guidebook for cyber-physical vehicle systems					
	ISO / SAE CD 21434	Road vehicles – Cybersecurity engineering					
	Others, please specify						
ECU software architecture	AUTOSAR	Automotive open system architecture					
	Others, please specify						
Other types of standards, please specify							

2.1.3 Rail

	Standards		Develop or observe	Apply standards in	Evaluate conformance by	Why apply	Why didn't apply
Safety	EN 50129 (IEC 62425)	Safety related electronic systems for signaling					
	EN 50126 (IEC 62278)	Reliability, availability, maintainability and safety (RAMS)					
	EN 50159 (IEC 62280)	Safety related communication in transmission systems					
	EN 50128 (IEC 62279)	Software for railway control and protection					
	Others, please specify						
Others, please specify							

2.1.4 Health

Standards			Develop or observe	Apply standards in	Evaluate conformance by	Why apply	Why didn't apply
Safety	IEC 62304	Medical device software - Software life cycle processes					
	IEC 60601 / 80601	Medical electrical equipment					
	Others, please specify						
EU medical device directive	Directive 90/385/EEC	Active implantable medical devices (AIMD)					
	Directive 93/42/EEC	Medical devices (MDD)					
	Directive 98/79/EC	In vitro diagnostic medical devices (IVDD)					
	Others, please specify						
Others, please specify							

2.2Your expectation on future standards

- What do you expect from the in-progress standards?
- What standards are still missing in your opinion?

		Standards		Content you expect or have interest
Under progress	Safety	IEC 62879 ED1	Human factors and functional safety	
		IEC 61508 ED3	Functional safety	
		ISO 20078	Extended Vehicle (ExVe) – web services	
		Others, please specify		
	Security	ISO/SAE 21434	Road vehicles -Cybersecurity engineering	
		Others, please specify		
	Safety Security Privacy co-engineering	IEC 63069 ED2	Framework for functional safety and security	
		Others, please specify		
	Artificial Intelligence, Machine Learning	ISO/IEC WD 23053	Framework for AI systems using Machine Learning (ML)	
		Others, please specify		
	Smart Manufacturing	IEC JWG21	Smart manufacturing reference model(s)	
		Others, please specify		
	Internet of Things (IoT)	ISO/IEC21823	Interoperability of IoT systems	
		ISO/IEC 30147	IoT – Methodology for Trustworthiness of IoT system/service	
		Others, please specify		
	Others, please specify			
Missing	Safety			
	Security			
	Privacy			
	S-S-P joint assessment			
	Others, please specify			
E.g.	***Under progress***	*S-S-P joint assessment*		*Ethical considerations w.r.t. highly automated systems*

3 Your usage of standards in building products or services

This section investigates standardized or proprietary methodologies for Safety, Security and Privacy engineering.

3.1Your products or services

The following subsections are oriented to organizations with certain roles, assuming that each SECREDAS participant plays one or multiple roles:

- **Section 3.1.1**: for S-S-P technology providers, e.g. Service or Research Institute, who apply S-S-P standards to develop Safety, Security and Privacy technologies, products or services.
- **Section 3.1.2**: for S-S-P technology integrators, e.g. OEM / Tier1 / Tier2 in auto industry, medical industry and rail industry, who apply the standards to specify S-S-P requirements or to evaluate the solutions which integrate S-S-P technologies.
- **Section 3.1.3**: for S-S-P evaluators, e.g. service or research institute, who apply the standards to provide consultancy, or to performs 3rd party assessment, qualification or certification.

3.1.1 For technology developers

The technologies listed below as examples are cited from SECREDAS D3.1 Initial Common Technology Element List. Compared to SECREDAS WP3 which is concerned with the partners' technology contribution to the project, this subsection aims to reveal the usage of standards in daily work of SECREDAS partners. Please feel free to complement the technologies listed in the following table.

- What technology, solution, service or product do you develop or research?
- What are their possible applications? E.g. vehicle sensing, vehicle connectivity, IVN, VCU, health, rail, etc.

	Type of your technology	**Possible application areas of your technology**
	Key distribution protocol	
	Cryptographic libraries	
	Hardware isolation technology	
	Hypervision technology	
	Secure elements	
	Secure OS / Trusted Execution Environment	
	Authentication and authorization	
	Identity management	
	Trusted anchor	
	Firewall	
	Certificate management	
	Differential privacy	
	Transport layer security	
	Distributed ledger technologies	
	VPN	
	Security or safety testing	
	Intrusion detection systems	
	Others, please specify (incl. proprietary)	
E.g.	*Secure OS*	*Security software stack in V2X, gateway in IVN*

3.1.2 For technology integrators

- In which product, solution or service do you integrate Security, Safety or Privacy technologies?
- What technologies do you apply or integrate for satisfying S-S-P requirements? E.g. hypervision, trusted anchors, TEE, secure elements, authentication & authorization, etc.

Area of your solution	Your product or service	S-S-P technologies you applied
Vehicle Sensing		
Vehicle Connectivity		
IVN & VCU		
Health		
Rail		
Others, please specify		
E.g. *Vehicle Connectivity*	*Telematics*	*Authentication & authorization*

3.1.3 For service providers

- What services do you provide on Security, Safety or Privacy?
- In which domain do you provide such services?

	Type of service	Your services	Applied domains
	Assessments		
	Testing services		
	Consultancy		
	Qualification / Certification		
	Others, please specify		
E.g.	*Assessments*	*Security analysis*	*Automobile infotainment systems*

3.2Your usage of methodologies, tools and models

3.2.1 Safety Security Privacy engineering methodologies

- What standardized or 3rd party or proprietary engineering methodologies or process are applied in your daily work for satisfying Safety, Security or Privacy requirements?

	Standardized	3rd party	Proprietary
Safety			
Security			
Privacy			
Other concerns, please specify			
E.g. *Security risk analysis*	*ISO 27005 – EBIOS based*	*N/A*	*In-house customized security risk analysis methodology for IoT systems*

3.2.2 Safety Security Privacy engineering tools

- What COTS or proprietary tools do you (plan to) apply to meet Safety, Security or Privacy requirements, and which properties the tools servers? The tools listed below are only examples. Please feel free to add any tools which interest you, including in-house ones.

		Software Tools	Safety	Security	Privacy	Other Concerns
	COTS tools	Ansys SCADE code generators				
		Cadence Automotive Functional Safety Kits				
		IBM Rational DOORS kit				
		Mentor Graphics Veloce hardware emulation platform				
		Parasoft C/C++test				
		LDRA tool suite				
		MathWorks Simulink				
		Other, please specify				
	Proprietary tools					
	Others, please specify					
E.g.	*COTS tools*	*MathWorks Simulink*	*X*	*X*	*N/A*	*N/A*

3.2.3 Safety Security Privacy models

- Do you use specific quantitative or qualitive Safety Security Privacy models?
- What purpose do the models serve in your work?

	Model	Purpose of usage
Security threat and risk modelling	STRIDE	
	OWASP	
	others, please specify	
System security engineering models	Cyber Resiliency Engineering Framework	
	others, please specify	
Other, please specify		
E.g. *Security threat and risk modelling*	*STRIDE*	*Security threat analysis in automotive IVN systems*

4 Your usage of standards in assessment activities

This section investigates your application of Safety Security Privacy assessment methodologies, either standardized or proprietary. Please feel free to add applicable methodologies, including in-house ones.

	Methodology	For self-assessment	For 3rd party assessment	For qualification / certification
Safety	FMEA (Failure Mode and Effects Analysis)			
	FTA (Fault Tree Analysis)			
	HARA (Hazard and Risk Assessment)			
	Others, please specify			
Security	Common Criteria			
	ISO 27005			
	EBIOS (Expression des Besoins et Identification des Objectifs de Sécurité)			
	SAHARA (Security-Aware Hazard Analysis and Risk Assessment)			
	HEAVENS (HEAling Vulnerabilities to ENhance Software Security and Safety)			
	STRIDE			
	OWASP Risk Rating Methodology			
	Others, please specify			
Privacy	NIST PRAM (Privacy Risk Assessment Methodology)			
	LINDDUN			
	Others, please specify			
Combined Safety Security Privacy methods *(incl. proprietary)*	AMASS (Architecture-driven, Multi-concern and Seamless Assurance and Certification of Cyber-Physical Systems)			
	AQUAS (Aggregated Quality Assurance for Systems)			
	Others, please specify			
Other concerns, please specify				
E.g. *Security*	*Common Criteria*	*X*	*X*	*X*

5 Open questions

5.1 On reuse and patterns

(1) As architect or designer or engineer, at which abstraction level do you consider reuse? E.g. domain-specific design or assets (i.e. platforms, items or products), domain-related architecture or asset architecture, safety/security/privacy reference architecture.

[Your Answer]

(2) What standards do you apply for improving the reusability at certain levels?

[Your Answer]

5.2 On quality assurance

(1) What is your impression on approaches to jointly consider safety-security-privacy?

[Your Answer]

(2) How do you obtain a cross-domain view in your development or research, so that your solution or product or service would work for various domains e.g. auto, rail and health?

[Your Answer]

(3) How do you maintain the safety or security level of your solution (product or service) during its evolution?

[Your Answer]

(4) What is lacking in the related standardization?

[Your Answer]

5.3 Other concerns or comments

[Your Answer]

www.secredas.eu

mail@secredas.eu

Social media @secredas.eu

Horizon 2020
European Union funding
for Research & Innovation

SECREDAS has received funding from the Electronic Component Systems for European Leadership Joint Undertaking under grant agreement nr.783119. This Joint Undertaking receives support from the European Union's Horizon 2020 research and innovation programme and Austria, Belgium, Czech Republic, Germany, Finland, Hungary, Italy, The Netherlands, Poland, Romania, Sweden and Tunis