2nd Annual review Florence 2013

WP6 – Platform Integration, Validation and Demonstration

Kyriakos Georgouleas (HAI)

WP6 - Tasks

- **T6.1 – Multi-Technology System Integration (HAI)**
  - Integration of components and prototypes
  - Demonstration of the interoperability of the various nSHIELD SPD modules
- **T6.2 – Multi-Technology Validation & Verification (SE)**
  - Specification of test procedure assessing interface compatibility
  - Validation of nSHIELD SPD fundamentals
  - Validation of integrated testbed
- **T6.3 – Lifecycle SPD Support (TECNALIA)**
  - Support the lifecycle of proposed solution
  - Conform with international standards (ISO/IEC 12207, ISO/IEC 15288)
  - Analyzing the security implications of upgrades

WP6 - Overview

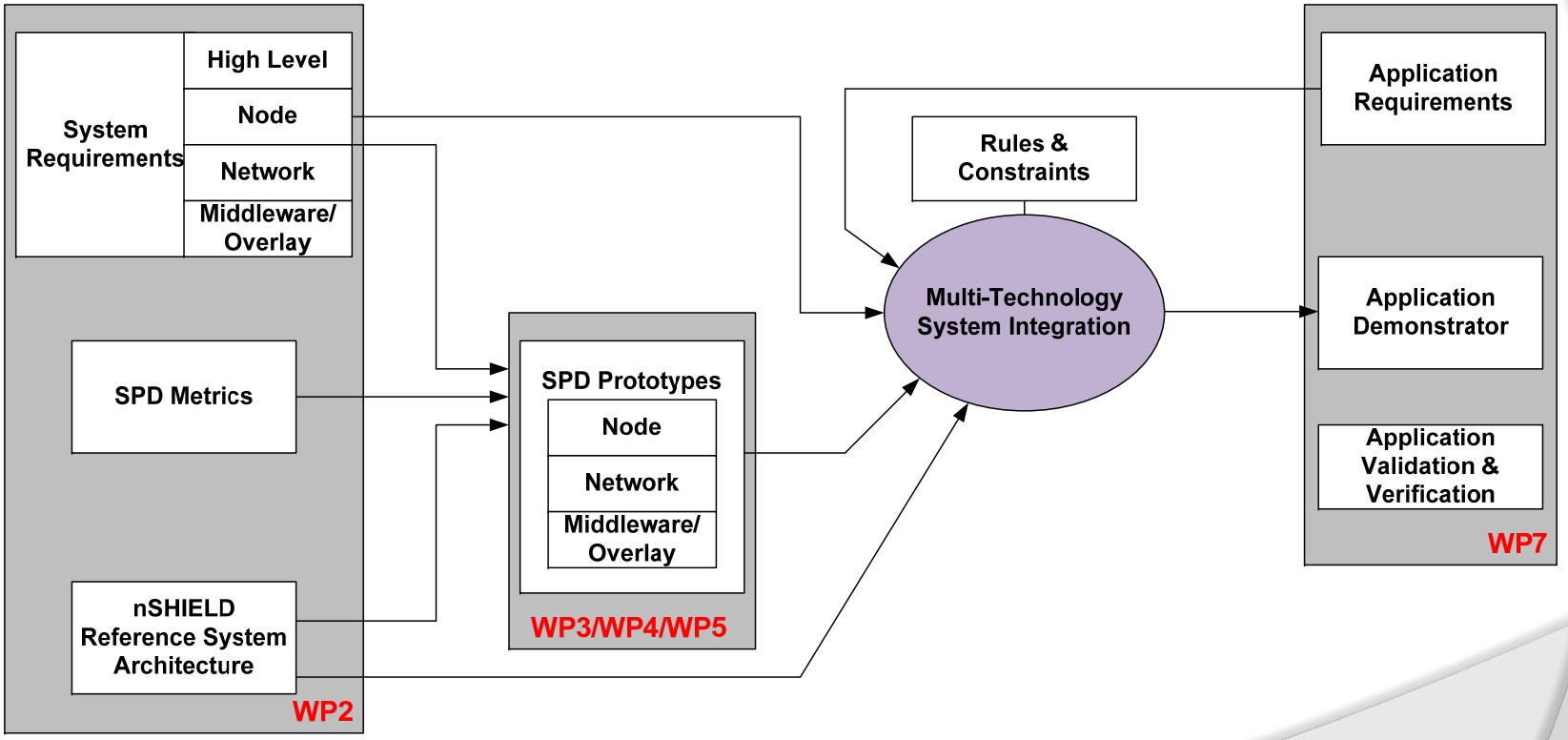
- Deliverables
  - D6.1, Lifecycle and SPD Support Plan (Internal, M18, finalized M20)
  - D6.2, Prototype Validation and Verification (Internal, M20, finalized M26)
  - D6.3, Prototype Integration Report (Internal, M22, finalized M27)
  - D6.4, Lifecycle and SPD Support Report (Public, M30)
  - D6.5, Platform Integration Report (Public, M34)
  - D6.6, Platform Validation and Verification (Public, M36)

Task 6.1 Multi-Technology System Integration

- Scope: compose seamlessly components and prototypes developed in WP3, WP4 and WP5 in order to address all SPD concerns and requirements of real application scenarios
- Relevance with Industrial Priorities
  - IP1 - Composability: *The ability to derive instantiations of architecture from a generic platform that support the constructive composition of large systems out of components and sub-systems*
  - IP2 – Architectural Dependability: *Architectural framework that supports the selection of the most appropriate SPD algorithms, technologies and procedures, development of the missing ones, and integration in a modular, composable, expandable and dependable way*

nSHIELD

Integration with work from other WPs



nSHIELD Prototypes (I)

Applications: 1. Railways Security
2. Facial/Voice Recognition
3. Reliable Avionic
4. Social Mobility

Prototype Number	Prototype name	Layer	Supported Platforms	Applications	Partner
0	Elliptic Curve Cryptography	ND			UNIGE
1	Lightweight Ciphering	ND	Memsic IRIS, BeagleBone, BeagleBoard	1,2,4	TUC
2	Key Exchange Protocol	ND	BeagleBone, BeagleBoard-xM		TUC
3	Hypervisor	ND	BeagleBoard-xM, BeagleBone, Integrator CP	1,23	SICS
4	Secure Boot	ND	BeagleBoard-xM, QEMU Simulator	1,2,3	T2D
5	Secure Power (&) Communication cape	ND	BeagleBone Cape	1	AT
6	Smart Card based Security Services	ND	SIM cards, Cryptographic SD cards	1,2,4	TUC
7	Facial Recognition	ND	Eurotech ANTARES, Intel Core i5, Linux or Windows	2	ETH
8	GPU accelerated Hashing	ND	GPU-equipped power nodes (e.g. Nvidia CARMA)	2,4	TUC
9	Smart Transmission	NW	OMBRA v2, SDR	3	SES/UNIGE
10	Anonymity & Location Privacy Service	ND	Zolertia Z1, BeagleBone, BeagleBoard, BeagleBoard-xM	2,3	TUC
11	Automatic Access Control	ND	BeagleBone, BeagleBoard, BeagleBoard-xM	1	TUC
12	DDoS Attack Mitigation	ND	Multi-core platform (FPGA, DSP, Linux, Windows CE, OMBRA)	2,3	ATHENA
13	Recognizing DoS	NW	BeagleBone, BeagleBoard, BeagleBoard-xM		ATHENA
14	Dependable Distributed Computation Framework	NW	BeagleBoard-Xm, ETH SecuBoard, server(s)	2	UNIUD
15	Intrusion Detection System	NW	Zolertia Z1	1	MGEP
16	Reputation-Based Secure Routing	NW	Memsic IRIS	1	TUC/HAI
17	Access Control Smart Grid	NW	SIM cards, Cryptographic SD cards		TECNALIA
18	Policy Definition	M		1	ASTS/SES/SESM
19	Policy Based Management Framework	M	Beaglebone, BeagleBoard-xM, BeagleBoard	1	TUC/HAI
20	Control Algorithms	O	CPN Tools	1,3	UNIROMA

nSHIELD

nSHIELD Prototypes (II)

Prototype Number	Prototype name	Layer	Supported Platforms	Applications	Partner
0	Elliptic Curve Cryptography	ND			UNIGE
1	Lightweight Ciphering	ND	Memsic IRIS, BeagleBone, BeagleBoard	1,2,4	TUC
2	Key Exchange Protocol	ND	BeagleBone, BeagleBoard-xM		TUC
3	Hypervisor	ND	BeagleBoard-xM, BeagleBone, Integrator CP	1,23	SICS
4	Secure Boot	ND	BeagleBoard-xM, QEMU Simulator	1,2,3	T2D
5	Secure Power (&) Communication cape	ND	BeagleBone Cape	1	AT
6	Smart Card based Security Services	ND	SIM cards, Cryptographic SD cards	1,2,4	TUC
7	Facial Recognition	ND	Eurotech ANTARES, Intel Core i5, Linux or Windows	2	ETH
8	GPU accelerated Hashing	ND	GPU-equipped power nodes (e.g. Nvidia CARMA)	2,4	TUC
9	Smart Transmission	NW	OMBRA v2, SDR	3	SES/UNIGE
10	Anonymity & Location Privacy Service	ND	Zolertia Z1, BeagleBone, BeagleBoard, BeagleBoard-xM	2,3	TUC
11	Automatic Access Control	ND	BeagleBone, BeagleBoard, BeagleBoard-xM	1	TUC
12	DDoS Attack Mitigation	ND	Multi-core platform (FPGA, DSP, Linux, Windows CE, OMBRA)	2,3	ATHENA
13	Recognizing DoS	NW	BeagleBone, BeagleBoard, BeagleBoard-xM		ATHENA
14	Dependable Distributed Computation Framework	NW	BeagleBoard-Xm, ETH SecuBoard, server(s)	2	UNIUD
15	Intrusion Detection System	NW	Zolertia Z1	1	MGEP
16	Reputation-Based Secure Routing	NW	Memsic IRIS	1	TUC/HAI
17	Access Control Smart Grid	NW	SIM cards, Cryptographic SD cards		TECNALIA
18	Policy Definition	M		1	ASTS/SES/SESM
19	Policy Based Management Framework	M	Beaglebone, BeagleBoard-xM, BeagleBoard	1	TUC/HAI
20	Control Algorithms	O	CPN Tools	1,3	UNIROMA

nSHIELD

Framework support for node capabilities assessment

Platforms	
1	Beagleboard
2	Beagleboard-XM
3	Beaglebone
4	Raspberry Pi
5	Arduino Uno
6	Zolertia Z1
7	Memsic Iris
8	OMBRA v2
9	Eurotech Secuboard
10	OMNIA
11	PC

Node Prototypes	
00	Elliptic Curve Cryptography
01	Lightweight Ciphering
02	Key Exchange Protocol
03	Hypervisor
04	Secure Boot
05	Secure Power (&) Communication Cape
06	Smart Card based Security Services
08	GPU-accelerated Hashing
11	Automatic Access Control
07	Face Recognition
34	Audio Surveillance System
30	Reliable Avionics

Network Prototypes	
09	Smart Transmission
12	DDoS Attack Mitigation
13	Recognizing DoS
14	Dependable Distributed Computational Framework
15	Intrusion Detection System
16	Reputation-based Secure Routing
17	Access Control Smart Grid
23	Link Layer Security
24	Network Layer Security
10	Anonymity & Location Privacy

Middleware/Overlay Prototypes	
25	OSGI Middleware
26	Semantic Model
18	Policy Definition
19	Policy Based Management Framework
20	Control Algorithms
21	Gateway
22	Middleware Intrusion Detection System
29	Legacy System Adapter
31	Middleware Protection Profile
32	Secure Discovery
33	Security Agent

nSHIELD

Prototypes supported by Platform

Platform Name: BeagleBone	Feature Supported	
	Yes	No
Physical Protection		
Custom Encapsulation	X	
TPM Crypto-coprocessor	X	
Secure power unit	X	
Secure Execution Environment	X	
Secure Boot	X	
Operating System		
Embedded Linux	X	
Communication Interface		
Ethernet	X	
USB	X	
Serial	X (add-on cape)	
SDR		X
802.11	X (add-on cape)	
802.15.4	X (add-on cape)	
RFID		
Smart Card		
Bluetooth		
Java Runtime Environment	X	
GPU Unit		X

Prototypes able to run					
Node Layer		**Network Layer**		**Middleware/Overlay Layer**	
00	*Elliptic Curve Cryptography*	24	*Network Layer Security*	25	*OSGi Middleware*
01	*Lightweight Ciphering*	12	*DDos Attack Mitigation*	26	*Semantic Model*
02	*Key Exchange Protocol*	13	*Recognizing DoS*	33	*Security Agent*
				32	*Secure Discovery*
				19	*Policy Based Management*

nSHIELD

Required Components for Application Scenario

Application Scenarios	
1	Railways Security
2	People Identification
3	Reliable Avionic
4	Social Mobility & Networking

Platforms	
1	Beagleboard
2	Beagleboard-XM
3	Beaglebone
10	OMNIA
11	PC

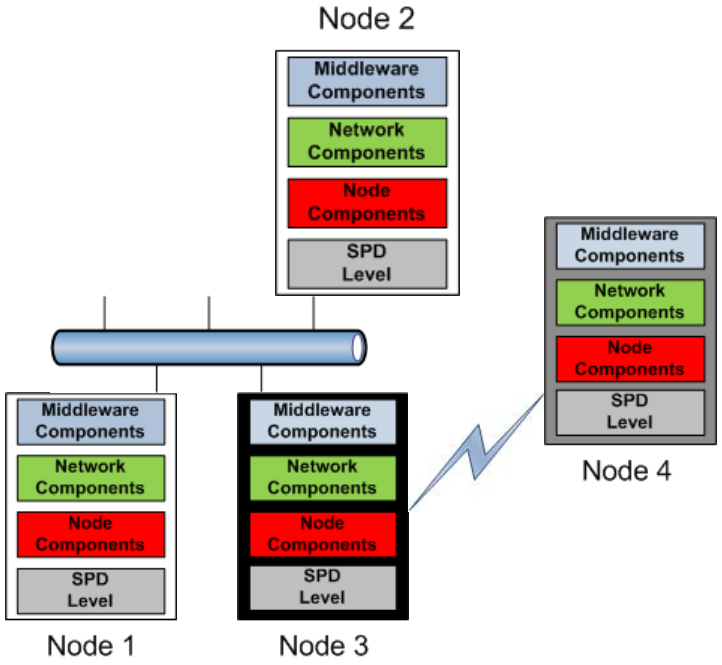
Node Prototypes	
00	Elliptic Curve Cryptography
01	Lightweight Ciphering
02	Key Exchange Protocol
03	Hypervisor
04	Secure Boot
05	Secure Power (&) Communication Cape
06	Smart Card based Security Services
08	GPU-accelerated Hashing
11	Automatic Access Control
07	Face Recognition
34	Audio Surveillance System
30	Reliable Avionics

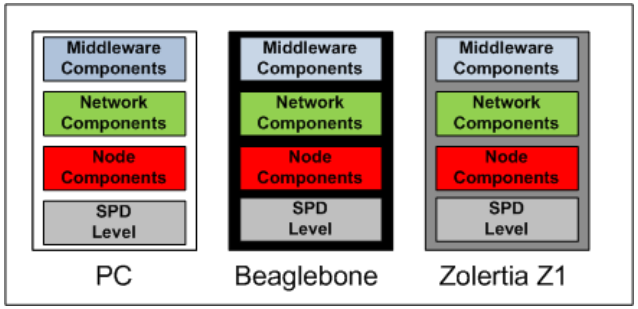
Network Prototypes	
09	Smart Transmission
12	DDoS Attack Mitigation
13	Recognizing DoS
14	Dependable Distributed Computational Framework
15	Intrusion Detection System
16	Reputation-based Secure Routing
17	Access Control Smart Grid
23	Link Layer Security
24	Network Layer Security
10	Anonymity & Location Privacy

Middleware/Overlay Prototypes	
25	OSGI Middleware
26	Semantic Model
18	Policy Definition
19	Policy Based Management Framework
20	Control Algorithms
21	Gateway
22	Middleware Intrusion Detection System
29	Legacy System Adapter
31	Middleware Protection Profile
32	Secure Discovery
33	Security Agent

nSHIELD

nSHIELD System Composition

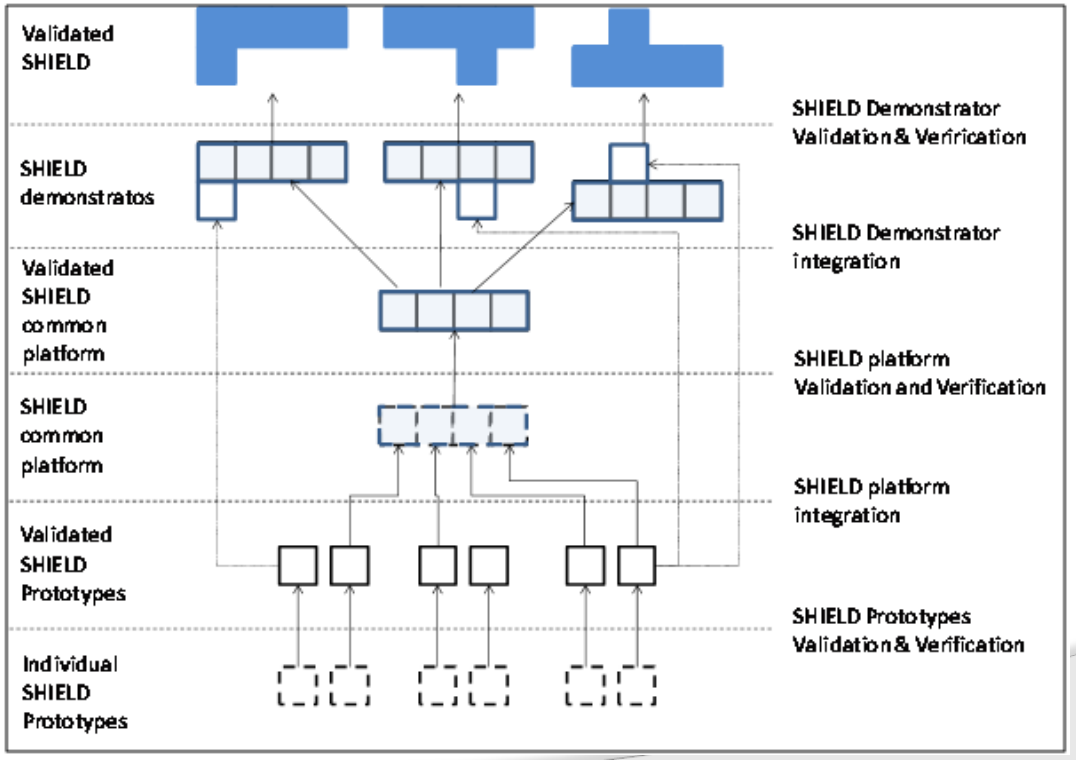




- Enable System Integrator view all Node/Network/Middleware components and SPD level of each device
- Enable System Integrator build integrated systems with all the components of the four application scenarios
- Enable System Integrator view all Node/Network/Middleware requirements fulfilled in the current configuration
- Composed system compliant with nSHIELD Reference Architecture

Task 6.2 Multi-Technology Validation and Verification

- D6.2 Prototype Validation and Verification: Focus on Validation and Verification of individual prototypes designed and developed in WP3/WP4/WP5



nSHIELD procedures for Validation and Verification

Means of Validation and Verification	
[A] Analysis	Dedicated Analysis
[D] Design	Specific design choice
[I] Inspection	Visual inspection of the element
[T] Test	Well described and documented test procedure
[R] Review	Review of project's documentation

Security evaluation methodology MEFORMA	
Preparation Phase	Establish test environment, threat modeling and specify exact steps of Evaluation phase
Evaluation Phase	Execute test cases defined in Preparation phase
Documentation Phase	Collect the findings of the Evaluation phase and perform risk analysis
Review Phase	Determine whether the threats identified during evaluation had been adequately addressed

Validation and Verification of nSHIELD prototypes

- Starting from the prototypes list and splitting them depending on their layer (node, network and middleware/overlay), validation and verification procedures for each prototype is included in D6.2

- The requirements (extracted from D2.2 Preliminary System Requirements and Specifications) addressed from each prototype have been analyzed together with their means of verification (A, D, I, T)

- Test procedures with exact execution steps have been developed for prototypes verified through testing

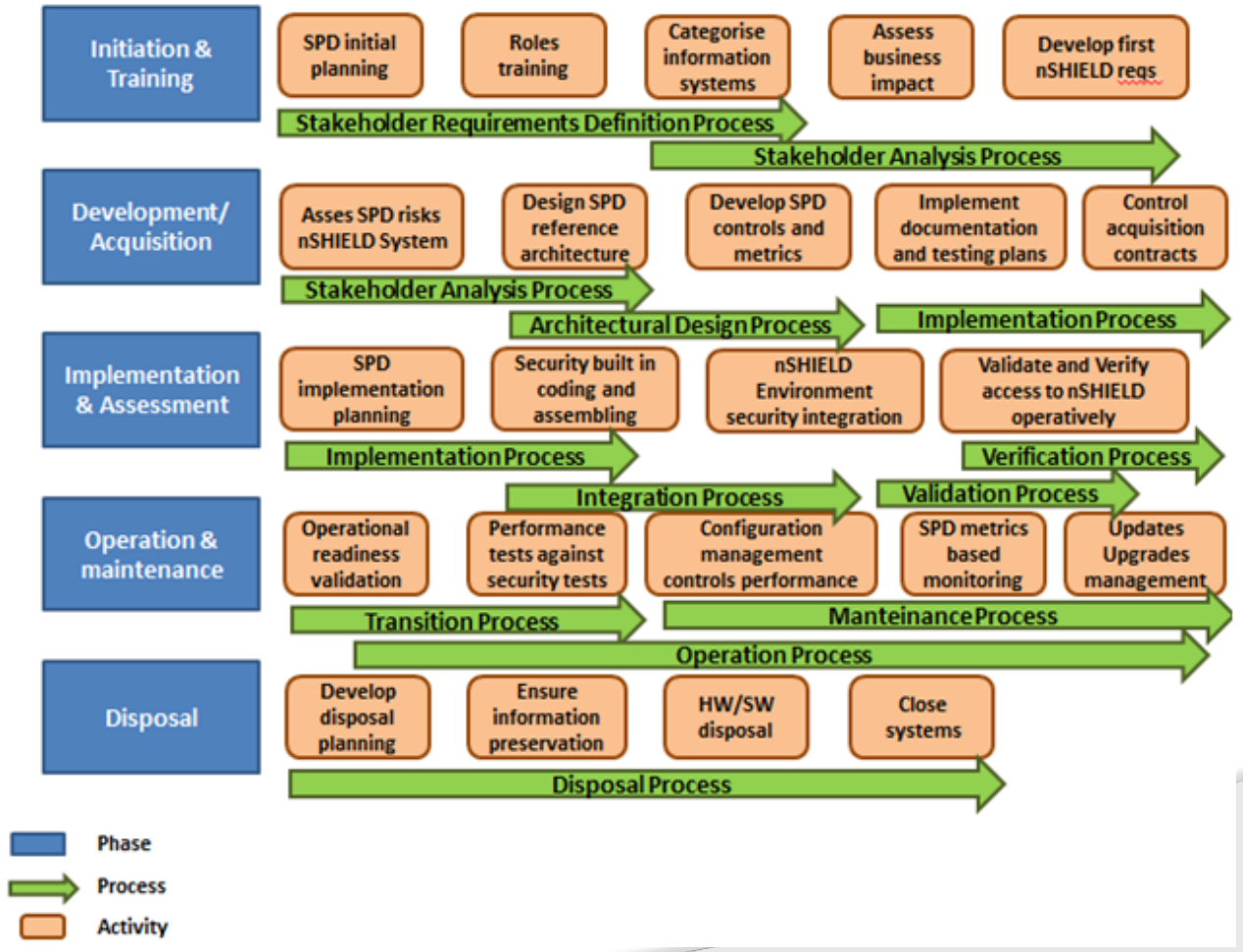
nSHIELD Test procedure format

Verification Test Nr.: 4.3.6.1	**Written by:** TUC	**Conducted by:**	**Date:**	**Test Category:** Network Security
Software and Hardware Configuration Details	• 3 Z1 sensor nodes • Nodes running Contiki OS 2.6 and the IPsec protocol with AES in CCM* mode. • PC running GUI application monitoring communication using a Sniffing node			
Test Name:	***Verification of confidentiality among communicated messages***			
Purpose:	Verify that the network layer messages are encrypted (REQ_NW01).			
Modules/Interfaces/Code Tested:	Network layer module IPsec module			
Step	**Action**	**Expected Result**	**Pass/Fail**	**Remarks**
1	Compile all nodes comprising the scenario. Only node 1 sends data packets in order to keep track of the communication.	-		
2	Switch on all nodes.	Network layer control messages are exchanged among nodes. Sniffer overhears all messages exchanged among the nodes.		
4	Start transmitting application-layer messages from node 1.	Packets exchanged between nodes are encrypted		
5	Switch off all nodes.			

Task 6.3 Lifecycle SPD Support

- SPD Lifecycle Principles in nSHIELD
- Security, privacy and dependability by Design
  - SPD design and architecture
  - Threat modeling and mitigation
  - SPD components design
  - Improvements in security incorporating legacy systems
- Security, privacy and dependability by Default
  - SPD Certification
  - Availability as core SoS atribute
  - System parameterization through nSHIELD metrics
- Security, privacy and dependability in Deployment
  - Deployment guides
  - nSHIELD control panel and management tools
  - Patch deployment tools

nSHIELD Lifecycle support methodology



Plan Execution

- Define a plan of how activities will be executed
- Activity elements of nSHIELD system defined in Plan Execution
  - Scope
  - Inputs and outputs
  - Synchronization towards nSHIELD system
  - Relations with standards
  - Measurements from SPD goals and SPD evidences
  - Guide for applicants
- Process description following ISO standards
- Execution of the plan will be delivered in D6.4 Lifecycle and SPD support report

WP6 Results and achievements

- Collection of all SPD prototypes, hardware platforms they run and assessment of their involvement in each one of the application scenarios
- Initial design of a framework for system composition of nSHIELD SPD components able to compose all defined application scenarios
- Validation and verification procedures for all nSHIELD prototypes (defined in WP3, WP4 and WP5 deliverables) as independent development efforts that meet the requirements defined in WP2
- Definition of the lifecycle support methodology for all the phases of nSHIELD development

WP6 Future Steps

- Development of a software tool for system composition of SPD components
- Composability tool able to support all defined and future application scenarios
- D6.5: Platform integration report
- D6.6: Validation and Verification of the integrated platform
- D6.4: Lifecycle and SPD Support Report

The END

That’s all folks!

ARTEMIS