

Digital Security and Privacy R&I Strategy



	LEIT-ICT	Societal Challenges
CNECT H4	<p>1. Dedicated Cross-Cutting Security R&I in LEIT-ICT: <u>Objective:</u> R&I on dedicated technology-driven digital security building blocks</p> <p>WP2014-15:</p> <ul style="list-style-type: none"> - Cryptography - End-to-end security <p>WP2016-17:</p> <ul style="list-style-type: none"> - Metrics, assurance and certification of security and/or privacy requirements 	<p>2. SC7 Digital Security <u>Objective:</u> Demonstrating the viability and maturity of state-of-the-art security, privacy and trust solutions; proving that security concepts, processes and solutions work in real life environment directly involving end users</p> <p>WP2014-15</p> <ul style="list-style-type: none"> - Privacy; Access Control; Risk management and assurance models - Role of ICT in Critical Infrastructure Protection - Information driven Cyber Security Management - Trust eServices; Value-sensitive technological innovation in Cybersec. <p>WP2016-17</p> <ul style="list-style-type: none"> - Cybersecurity for all - Solutions addressing targeted, combined cyber and physical threats against European infrastructure and enterprises - Privacy; – Ethics
Others	<p>3. Mainstreaming in LEIT-ICT <u>Objective:</u> Ensuring security as a functional requirement in specific technology R&I:</p> <ul style="list-style-type: none"> - Embedded systems, ICS security - Components/micro-electronics - IoT, future internet/5G - Cloud - Big Data - Software Engineering 	<p>4. Mainstreaming in other SC1, 3, 4, 6 <u>Objective:</u> Ensuring digital security integration in the application domains and in complex systems integration:</p> <ul style="list-style-type: none"> - eHealth – privacy and security aspects of medical devices/apps - Energy (smart grids, smart meters) - Transport (including ITS) - Innovative security solutions for public administration and co-creation - Resilience of multi-sector systems (e.g. smart cities)