

Proposal Acronym	VERIFY
Proposal Title:	New methods for verification of security and privacy mechanisms in e-commerce and e-government systems
Surname:	Derek
First name(s):	Ante
Research area:	Information science and Engineering ENG
Sub-discipline of research area:	Complexity and cryptography, electronic security, privacy
Category of research:	developmental
[REDACTED]	[REDACTED]
Abstract:	<p>Usage of computer systems and networks in government, education, healthcare and almost every other aspect of everyday life has produced an abundance of sensitive digital data across various digital archives and services. Sensitive data includes not only personally identifiable information but also any piece of information whose misuse (unauthorized access, sharing, publication or correlation with other data) can harm the data subject. Such data is almost never physically or logically isolated from the rest of the world - it is usually partially exposed via interfaces such as web services or interoperability with other digital systems or services. For example, computer system for enrolling students in universities may interface with central school system to retrieve students grades or test results, interface with government systems to confirm students address or citizenships etc. While the security and privacy issues concerning isolated or homogenous systems are somewhat well understood, growing interoperability of heterogeneous computer systems is rarely accompanied with systematic investigation of security and privacy properties provided by the resulting system as a whole. The goal of this research is to develop new methods of specification and verification of security and privacy properties of the heterogeneous interoperable computer systems that handle sensitive data and expose it through public or private interfaces.</p>
Does this proposal possess any of the sensitive ethical issues detailed in ethical issues table?:	No