**MSc project descriptor**

Industrial mentor contact details (including name, address, email, telephone):

Gavin Davis, [gavin.davis@leonardo.com](mailto:gavin.davis@leonardo.com)

Crewe Toll Phase 2, 2 Crewe Road North, Edinburgh EH5 2XS.

Project Title

Privacy-aware digital signing for device identification

Project Description

In this project, we will investigate the benefits of using trusted devices to digitally sign transactions using an anonymous digital signature, but where it can still be trusted. Key technologies include Zero Knowledge Proofs and Privacy-aware Signatures.

This project will provide insight on the following questions:

* How can we manage keys in a highly distributed network?
  + How do we revoke and regenerate/distribute keys in the event of a key becoming compromised?
  + How can we manage key refresh cycles? Especially when it is not viable for assets to return to base for refresh.
* How can we identify new assets on the network and authenticate/identify them?
  + How can new assets on the network be identified without relying on a centralised trust store?
  + How can once trusted assets be removed from the network if they are compromised?
    - How can we both prove the origin of a message while protecting its contents from malicious actors?
  + How can authorisation of access to assets be controlled?
    - How can we know that a legitimate asset has the correct authorisation to communicate with another asset?

Key Objectives

The objectives of these project are to provide:

* A comparison of current technological solutions with a focus on:
  + The theoretical background of the solution
  + Pros and cons of the solution
  + Barriers to adoption for the use case outlined above
* Prototype solution(s) to demonstrate the technologies and analyse performance.
  + Identifying the strengths/weaknesses of the solution and areas of further improvement
* A make/buy proposal
  + Are there existing solutions that we can adopt, or do we need to build our own solution based on the theory?
* Identify any gaps in the work presented and areas of future work.