Innovate UK
Technology Strategy Board

Results of competition:

Making remote working secure, resilient and reliable - Collaborative R&D

Total available funding for this competition was £3.5m from Innovate UK.

Note: These proposals have succeeded in the assessment stage of this competition. All are subject to grant offer and conditions being met.

Participant organisation names	Project title	Proposed project costs	Proposed project grant
Avanti Communications Limited (lead) Quortus Limited	VOLANS: Secure, Resilient and Reliable 4G with 3G/WiFI/SIP Mobile Network Access for Remote Users	£581,015	£348,609
Project description - provided by applicants			
Project VOLANS will develop a multi-technology combining 4G with either 3G / WiFi / SIP software core network operable in a cost-effective hardware platform for remote deployment.			

Innovate UK
Technology Strategy Board

Results of competition:
Making remote working secure, resilient and reliable - Collaborative R&D

Note: These proposals have succeeded in the assessment stage of this competition. All are subject to grant offer and conditions being met.

Participant organisation names	Project title	Proposed project costs	Proposed project grant
Evidentia Limited (lead) University of Kent	Authenticated Self - The "aS" Platform	£395,508	£283,688
Project description - provided by applicants			
While there is pent up demand for a reliable alternative to user passwords in SMEs working with sensitive and commercial information, there is news everyday of security breaches, cyber-attacks & data compromises. To compound the issue, many employees use personally owned devices to access work systems which increases the risks. The proposed authenticatedSelf “aS” platform seeks to resolve the factors that breach security by reliably authenticating that the person accessing the system is who they purport to be. We will target the diverse SME community where there is heavy use of remote IT and those organisations most vulnerable to attack/vulnerability of remote working. The project will use employees' personal Smart Phones which will only grant access to secure systems when they detect a number of worn NFC tags in close proximity. The requirement for a certain number of close by tags in association with energy efficient security protocols will address the above problems.			

Innovate UK
Technology Strategy Board

Results of competition:
Making remote working secure, resilient and reliable - Collaborative R&D

Note: These proposals have succeeded in the assessment stage of this competition. All are subject to grant offer and conditions being met.

Participant organisation names	Project title	Proposed project costs	Proposed project grant
iProov Limited (lead) Media Research Partners t/a The Media Institute	VASOCISE - Visual Authentication for Secure Online Control in Small Enterprises	£497,389	£288,458
Project description - provided by applicants			
Project VASOCISE addresses a core challenge for SMEs today - how to create a secure environment for staff who frequently are working from home, part-time, on site or travelling, whilst not creating an intolerable burden of cost, complexity and unenforceable rules. The project builds on iProov's highly useable zero-effort authentication technology to create a zero effort access solution for SMEs, tightly controlling access to their systems and their data in a highly useable way. VASOCISE also addresses the complexity of implementation and management, with some highly innovative solutions to make these so simple for SMEs that the threshold of adoption can be crossed, and the data of staff, management and customers can be protected.			

Innovate UK
Technology Strategy Board

Results of competition:
Making remote working secure, resilient and reliable - Collaborative R&D

Note: These proposals have succeeded in the assessment stage of this competition. All are subject to grant offer and conditions being met.

Participant organisation names	Project title	Proposed project costs	Proposed project grant
Nquiringminds Limited (lead) Impleo Professional Services Limited University Of Oxford	SECD- Secure Enterprise Companion Device	£676,518	£453,474
Project description - provided by applicants			
The SECD addresses the fundamental paradox posed by BYOD: how do you secure data when you no longer have control of the device. A BYOD roll out gives employees a free choice on device type, operating system and configuration. It is impossible to universally secure such a diverse device set: portable software only solutions are susceptible to rooting attacks; fully defined hardware stacks (like Samsung KNOX) are no longer BYOD as the device is now fully specified. SECD will address this problem by defining a hardware hardened, tamper proof companion device based on state of the art Trusted Computing principles. This device will serve applications "locally" to the employee's device over web, augmented by secure web extensions to be made available in a trusted enterprise web browser. This solution will be evaluated across a number of companion devices including SIM card, USB dongle and MIFI solutions. This device will not only serve applications, but will cache encrypted data, mediate network connections, and also provide enhanced multi factor authentication for user identity. With SECD employers retain total control of their data, but employees can access it flexibly.			

Innovate UK
Technology Strategy Board

Results of competition:
Making remote working secure, resilient and reliable - Collaborative R&D

Note: These proposals have succeeded in the assessment stage of this competition. All are subject to grant offer and conditions being met.

Participant organisation names	Project title	Proposed project costs	Proposed project grant
Seven Technologies Group Limited (lead) Queens University Belfast	IMES (Intelligent Multifactor Endpoint Security)	£743,944	£504,042
Project description - provided by applicants			
The Intelligent Multifactor Endpoint Security (IMES) system brings high security connectivity to remote workers in an affordable, intelligent and easy to use solution. Designed to address the security challenges of Remote Working and BYOD it introduces innovative multi-factor authentication requiring minimal input from the User. Three factor Authentication is provided by: LIOPA Speaker Verification technology to establish liveness and biometric characteristics of the User; An Authentication Service pairs autonomously with a low Energy RF token; and a profiling service checks User metrics (working pattern, device identity and network connectivity). Once authenticated Users connect through a local Proxy server which provides a 'CleanWeb' whitelist for safer browsing or through to their nominated Endpoint resource. The VPN service is available for IOS, Android and Windows supporting PPTP, OpenVPN SSL, and L2TP/IPsec. DNS traffic is encrypted removing the risk of 'Man in the Middle attacks' typical with BYOD hardware. The VPN Service protects the User's privacy from local or remote interception over shared networks and protects their geographic location from the wider internet.			

Innovate UK
Technology Strategy Board

Results of competition:
Making remote working secure, resilient and reliable - Collaborative R&D

Note: These proposals have succeeded in the assessment stage of this competition. All are subject to grant offer and conditions being met.

Participant organisation names	Project title	Proposed project costs	Proposed project grant
Thales Research & Technology (UK) Limited (lead) HW Communications Limited Trustonic Limited	Secure Proxy for Information assurance using TrustZone - SPITZ	£731,658	£400,339

Project description - provided by applicants

We propose the development of a secure platform to enable remote working on untrusted (BYOD) user devices. We will show how an untrusted (BYOD) device can be used as an ultra-thin client in combination with a trusted intermediary (mobile wiifi like) device to provide secure access to company IT systems.

Our solution uses an innovative combination of TrustZone security functionality and remote / virtual desktop software in a trusted device with an ultra-thin client app running on the untrusted user device. This combination ensures that no company data is stored on the untrusted device and that access to the company network cannot be gained from the untrusted device.

Many previous attempts to provide trusted BYOD for sensitive workers have foundered due to their reliance on special hardware or feature integrations in the untrusted device itself, which severely limits choice and value of the BYOD aspect.

This project solves that problem whilst bringing more reliable security. The consortium comprises Thales UK Research and Technology, Trustonic Ltd and HW Communications Ltd.

Innovate UK
Technology Strategy Board

Results of competition:
Making remote working secure, resilient and reliable - Collaborative R&D

Note: These proposals have succeeded in the assessment stage of this competition. All are subject to grant offer and conditions being met.

Participant organisation names	Project title	Proposed project costs	Proposed project grant
Thinking Safe Limited (lead) 2iC Limited De Montfort University Royal Holloway University of London University of Warwick	Secure Remote Working in the Supply Chain (SeReWiSC)	£517,000	£355,000

Project description - provided by applicants

This project will allow remote workers to securely access information and control equipment, which is owned and operated by multiple organisations, supporting secure and flexible collaboration between people distributed across multiple organisations in the supply chain, using infrastructure from multiple suppliers.

Organisations need to ensure users and devices only access information and equipment in accordance with defined policies, need to ensure policies can be defined by business people that understand the commercial implications of the policies, and need to ensure timely and effective response to perceived risks and threats, with particular attention to the legal, social and ethical contracts between people and organisations.

Users need to support multiple organisations and groups, using the same devices for all, but ensuring the information and controls remain separate, recognising their role in the security of those organisations.

The solution combines user experience considerations with technical security controls and third-party integrations, creating a coherent, secure, flexible and easy to use solution for the whole supply chain.

Innovate UK
Technology Strategy Board

Results of competition:
Making remote working secure, resilient and reliable - Collaborative R&D

Note: These proposals have succeeded in the assessment stage of this competition. All are subject to grant offer and conditions being met.

Participant organisation names	Project title	Proposed project costs	Proposed project grant
Tracline (UK) Limited (lead) EE Limited Fujitsu Services Limited University of Surrey Mountsides Limited	Managing Communication Channels for Reliable Remote Working - Project 'Grand Union'	£614,071	£397,520

Project description - provided by applicants

The ‘Managing Communication Channels for Reliable Remote Working’, or Grand Union, Project is a 15-month collaborative industrial research activity into ‘Making Remote Working Secure, Resilient and Reliable’.

The aim of the project is to seamlessly improve the interoperability and increase the resilience of remote services across Wifi, WiMax, 3G/4G and future 5G networks. The key objective of the Project is to evaluate the capability of the new technology using pilot demonstrators deployed for the mobile workforce of an SME that is supporting the healthcare sector.

The primary innovations are provision of:

1) A simple to understand network QoS/GoS/User Experience indicator plus access to a single integrated, comprehensive network utilisation statement irrespective of the number of actual network providers used;

2) Integrated TCP/IP Accelerator, delta caching and persistence to improve data transfer efficiency and reliability across wireless networks.

The primary benefit of this new approach is that mobile workers will have significantly improved reliability, efficiency and resilient data network access with substantial, detailed and simple to understand evidence about their network access. The partners have initiated a comprehensive strategic planning process utilising Gantt charts (appendix B) and other suitable planning methods to ascertain the specific work packages and

required person days necessary by each partner assigned to the project. A comprehensive analysis has also been prepared of current equipment highlighting areas where additional capital expenditure is required to complete the project.

The cost projections are therefore felt to be both prudent and accurate and the project management team is confident of being able to deliver the project within budget and within the forecast timescales.

Total Partner costs for this Industrial Research Project are £617k with the project spanning fifteen months. Total contributions from the partners will be £315k with the collaborators seeking the remaining £302k from Innovate UK funding, additional information regarding each partner's commitments are provided within the 'Finance Summary Table'. Initial assessment of the key project deliverables and milestones has been made by the project partners; this has resulted in the following cost calculations being established:

- Internal labour costs will be by far the most significant element, representing ~69% of the overall expenditure estimated at £428k, with an overhead recovery applied at 20% as determined by Innovate UK in order to simplify the overhead calculation process, the total overhead cost will be £85k (~14%)
- Full Time Sub-contractor Pawel Weclawiak has an existing relationship with Tracline and will provide an integral part of the project development and continuity to Tracline's projects, constituting 5% of the overall cost £30K. (See App C3).
- Overheads, various other accumulated costs £18k (~3%) which include initial IPR investigations into the novel aspects of the technological solutions.

With the level of resources specified the key objectives of this Project will be completed in the targeted time frame and the outcome of the 'Grand Union' Project will be a pilot demonstrator providing a major step forward in the security, resilience and reliable connectivity of mobile communications for remote working.

Innovate UK
Technology Strategy Board

Results of competition:
Making remote working secure, resilient and reliable - Collaborative R&D

Note: These proposals have succeeded in the assessment stage of this competition. All are subject to grant offer and conditions being met.

Participant organisation names	Project title	Proposed project costs	Proposed project grant
Xuvasi Limited (lead) Alazen Limited Paradigm Agnostic Limited University of Glamorgan	Roost: Intelligent Information Storage with Granular Security	£622,851	£420,567
Project description - provided by applicants			
Roost provides an intelligent information storage system that leverages existing remote storage services, such as DropBox, etc., to provide SMEs with a Virtual Data Aggregation layer for use across their business. Roost incorporates a number of key innovations that work collaboratively to deliver increased resilience and information security at the same time as maximising the potential for SME staff to access and make use of permitted information that helps them to be more effective and efficient. Roost is being designed to deliver affordable, effective, and intelligent information storage that helps SMEs concentrate on their business rather than on managing numerous external storage providers.			