Secure Information Sharing Challenge

Truly Reliable and Unquestionably Secure Technology Challenge (TRUST)

1. Challenge topic

The Secure Information Sharing topic will address the necessity for trusted exchange of information between organisations using zero-trust principles with a focus on the Confidentiality, Integrity (trust), and Availability of streaming data (CIA triad).

.

2. Background

We live in a digital age defined by our dependence on the internet. As both compute power and network bandwidth increase, we are seeing a growth in applications that require the near real-time streaming (as opposed to sending static files) of video, audio, text, and other data.

Protecting streaming data from theft, tampering, eavesdropping, and obfuscation is essential, however, this can be very difficult. Data security for streams (i.e. securing the data itself, not the network channel) must be assured over open networks (e.g. 5G/6G), operate in near real-time without significant added latency, impose minimal additional compute burden and – in some cases –be usable in highly distributed and/or remote applications which tend to have significant constraints on power and form factor (e.g. IoT, augmented reality headsets, operations in the high north, etc.).

This Challenge seeks to develop both software and hardware solutions that provide CIA for highly dynamic, streaming data with an emphasis on ensuring trust in the data being shared across heterogeneous organisational boundaries through unsecure networks including the use of data centric security techniques and technologies. Furthermore, we challenge companies to develop methods to ensure the veracity of streaming data throughout the data lifecycle, from the point(s) of collection or creation to the point(s) of consumption. Finally, we are seeking innovative solutions that provide alternatives to common commercial tools for lightweight, user-friendly federated text, voice, and video chat on personal or organisation-provided mobile devices so that, for example, the location, identity, and communication patterns of chat participants are not discoverable by third parties.

DIANA is particularly interested in solutions that support highly distributed and resilient IT architectures building on capabilities currently being developed for the finance, supply chain, healthcare, gaming, content creation and distribution, and other commercial industries.

3. Technology Challenges

DIANA is seeking disruptive capabilities in the following areas:

3.1 *Confidentiality:*

This refers to the ability of a system to ensure that information can only be accessed by authorised users. DIANA seeks novel solutions that:

1. Provide quantum-safe protection of streaming data from the point where data are created or captured through to where the data is consumed;
2. Enable protected streaming data to be safely transmitted on unsecured networks (e.g., 5G / 6G) and viewed or manipulated on untrusted devices;
3. Support data streams that contain multiple components (e.g., audio, video, streaming text) where the components can be encrypted separately, and where the encryption keys for the entire stream or any stream component can be modified dynamically during data transmission to selectively enable /disable access by consumers based on their access rights;

3.2 ***Integrity:***

Consumers of data must have assurance that the data originated from a trusted source, has not been altered, and is accurate. DIANA seeks novel solutions that:

1. Support federated and distributed authentication and authorisation of users & devices using zero-trust principles across unsecure networks;
2. Provide non-repudiation of data especially from IoT devices deployed in public places;
3. Can detect altered / generated video or audio in near real-time (e.g., deep fake detection);
4. Allow organisations to provide full non-repudiation of digital streaming content.

3.3 ***Availability:***

Organisations must ensure that data at rest and in transit is robust against system failures, environmental conditions, or malicious activities. DIANA seeks novel hardware and software solutions that:

1. Are highly resistant to electromagnetic interference or other forms of jamming;
2. Provide reliable bandwidth, data quality, and connection stability when used in challenging environments (e.g., extreme latitudes, under water, dense urban environments, etc.);
3. Provide levels of redundancy appropriate to the application's objectives (e.g., mesh networking for IoT devices);
4. Support the prioritised transmission of data over low-bandwidth networks;
5. Automatically adjust stream data rates to fit with existing network bandwidth;
6. Can seamlessly utilize multiple redundant and diverse network paths simultaneously;
7. Demonstrate novel and disruptive use of advanced 6G wireless network infrastructure.

Other novel approaches for ensuring CIA of streaming data that provide capabilities not mentioned above will be considered. The T.R.U.S.T Challenge team aims to create a balanced portfolio that includes extremely disruptive solutions at lower TRL (as low as TRL-4) to more mature solutions (TRL 7-9) that are currently disrupting over industry sectors and need only be adapted for defence use.

4. Deliverables (6 months for phase one, with potential for an additional second phase of 6 months)

The challenge programme will be split across two phases of six months, with advancement to the second phase being a result of tangible and demonstrable progress in the first. Deliverables should show considerable progress and clear development potential at the end of phase one, with phase two outputs providing sufficient demonstration of capability to attract further, onward, scale-up and development investment from entities other than DIANA.

Strong candidate solutions will:

- Clearly address the problem(s) to be solved;
- Demonstrate new capabilities (or performance increases) that are disruptive;
- Can be easily scaled;
- Offer reliable, easy to maintain, robust, and (ideally) cost-effective solutions;
- Significantly increase the confidence and trust people have in streamed data;
- Allow for compatibility and interoperability with other communication technologies.

Furthermore, we are looking for proposals that:

- Describe the technology developments and timeline needed to deliver the innovation;
- Make effective use of the funding available to progress the technology proposed; and
- Cite specific civilian or commercial applications and defence benefits, where known .

By the end of the programme, the capability must contribute – plausibly and significantly – to the advancement of a solution and should be characterised by genuine innovation in the market. Existing commercial, off-the-shelf technologies will not be considered unless a novel modification is proposed.