Team Defence Information

Joint MOD/Industry Collaborative Working Environment Project Launch – 25 April 2024

Compiled by Tony Butler

Why?

The purpose of this briefing note is to agree a representative Industry view on collaborative working between partners across the Defence enterprise from MOD and front-line users to prime contractors, SMEs and individual users in the Defence supply chain. To date, a proliferation of Collaborative Working Environments (CWEs), bespoked to individual platforms or capabilities with little thought given to coherence, has led to limited re-use, avoidable costs and SMEs reluctant to invest in multiple collaborative workspaces. Furthermore, without standardisation, useability has been inconsistent and interoperability/integrateability remain unaddressed. Similarly, the supporting marketplace for CWEs has grown piecemeal in response to stove-piped business needs and is considered to be unsustainable for Defence users.

Team Defence Information (TD-Info) is facilitating the initial stages of a longer-term project to cohere demand for a generic collaborative working capability. The project intends to coalesce agreement covering technical, environmental, procedural and business characteristics that may be applied to CWEs in Defence and supported by a demand-led ecosystem. Within these, the project will consider:

- Scope - examine existing capabilities in-use in MOD and Industry and draft a user requirement for CWEs working at SECRET (including caveats) and OFFICIAL. This workstream will define what is meant by CWE (noting there may be more than one)
- Service Approach – follow ITIL with understanding developed from existing CWEs and from previous learning (qv TD-Info's Secure Information Sharing (SIS) URD/SRD, IDAM project and Transglobal Secure Collaboration Programme (TSCP) drivers)
- Ecosystem/marketplace – a commercial framework to enable suppliers to build workable, secure, collaborative systems for users – take soundings from CCS, DE&S and Commercial X. Implied tasks include business drivers – and business benefits – for users in addition the business opportunities for vendors
- Methodology – coherent (granular[1]) architectural approach – follow MODAF/TOGAF views. Develop from existing good practice (eg SIS URD/SRD)
- Compliance – critical workstream to incorporate legal and technical governance including assurance and accreditation for international working – eg SbD, EGADD
- Ease of Adoption – where appropriate exploit existing capabilities such as JOSCAR, Exostar, MAG, IDAM and other collaborative toolsets to establish trusted relationships

The drivers for this project are to better support future collaborative working capabilities in order to improve performance, optimise existing and planned investments and work towards a standardised approach. The additional benefits from aligning contracts and

[1] CWEs built using proven elements – eg IDAM or gateways – rather than starting from first principles.

managing confidentiality and privacy measures in a common way will be felt equally by MOD and Industry.

What?

CWE Requirement – Statement of User Need[2] (SUN):

Defence must have reliable, readily deployable and secure methods of working together with its industry partners, suppliers and partner organisations that are based on sharing information that is relevant, timely and accurate using controlled and auditable methods both within and across organisation boundaries.

The drivers for a capability to meet the SUN above remain valid for the purposes of this project; Existing technical options may offer immediate solutions for CWEs; however, the following criteria should be considered as the baseline for any future, generic, CWE capability:

- Project scope includes working at SECRET and OFFICIAL (including O-S).
- Meets information exchange needs of users
- Satisfies governmental security criteria (including caveats and export control measures) of all relevant, national, bodies and protects Industry IP
- Delivers improved efficiency and demonstrable value-for-money (vfm) for Industry and MOD users
- Enables granular management of identities (individual and organisational) and rights access
- Delivered as a service (which may be on-premise or in secure cloud)

The project envisages a range of CWE components that may be used in combination to deliver a collaborative working capability that reliably and cost-effectively meets the user need.

A range of candidate systems were reported by the workshop. Although some are, for the moment, limited to working a <S, all have utility and may make a worthwhile contribution to the Defence CWE inventory. A sample is listed below (others will be added as the project develops):

- BlueJay
- CasNet
- Hermes
- Rosa
- Galaxkey
- Slack
- Kahootz
- …
- (plus SDA components from Oracle etc)

[2] From SIS URD – DES CIO/14/3/59/07 dated 14 June 2013 – CWEs are of equal value to MOD and Industry - recommend replacing '*with its*' at the end of line 1 with '*between MOD,*'. SSUN to be agreed in consultation with MOD sponsor.

In addition, the envisaged CWE capability framework is to be delivered via a supporting commercial ecosystem in which competition is encouraged within a trusted marketplace that is incentivised to maintain industrial best-practice and vfm.

Benefits

Part of the project intent is to identify the whole-life benefits anticipated by the approach taken and to define measurable success criteria that satisfy investment decisions. The project should also highlight where opportunities to enhance collaborative working resulting from changes to policy may be considered by the authority's risk management function. By improved awareness of currently fielded CWEs[3], the project intends to minimise technical risk and discourage the proliferation of CWEs across the enterprise. In addition to improving vfm for CWE users, the intended end-goal is for improved, interoperable collaboration to enable projects and platforms to deliver faster and cheaper.

A key objective for this project is that the MOD SRO or Industry lead should have a clear and consistent description of CWE services across several dimensions - service description, comme rcial model etc. The working group will explore each of these to improve coherence, consistency, clarity and confidence when buying CWE services.

Who/How?

The project is co-chaired by two experienced, independent Defence business executives with guidance (and governance) from MOD Stratcom (DD). Facilitated by TD-Info, the team will comprise volunteer subject matter experts from member organisations and augmented by MOD staff as determined by the MOD sponsor.

The project will produce a detailed stakeholder map for the capability user group and a separate set of, potential, suppliers to make up the initial CWE ecosystem. At the highest level, the stakeholders may be grouped as follows:

- UK Government (MOD and DE&S)
- Other-nation governments (DoD/MOD level)[4]
- UK Industry (DSF, Defence SMEs)
- Non-UK Industry supporting international projects (eg GCAP/AUKUS)

Next steps:

- Support MOD SRO in preparing CWE plan for presentation to MOD Capability Board
- Establish teams to deliver CWE project workstreams
- Agree draft SSUN (limit by filtered range of capabilities taken from SIS URD/SRD)
- Identify existing CWE capability (understand marketplace – cf stocktake in DE&S)
- Produce WG ToRs (with RoE)
- Produce detailed plan – with timings

[3] The project additionally notes the Secure-by-Design imperative for systems handling MOD data
[4] Engagement with non-UK officials, where appropriate and necessary, will be managed by MOD.

- Research existing metadata standards and taxonomy(ies)

Assumptions:

- This project is focused on aligning demand and setting a framework for future CWE capability. Existing CWEs will be unaffected
- Service-provision (rather than equipment-based solutions)
- Existing service catalogues may be used to spread awareness of CWE capability (eg CCS)
- SbD processes may support authoritative international working
- Existing metadata standards and taxonomy(ies) may be applied by CWE WG
- DLOD approach – particularly for interoperability and integration (consistent with BMfS/Integration Design Authority) and Doctrine to ensure that risks and opportunities are considered with rigour and referenced to investment choices
- Sovereign approach – support UK businesses

Risks/Threats:

- Security aspects as a consequence of changed approach to joint CWEs (technical and personnel)
- SbD proves not to be authoritatively equivalent to accreditation requirements observed by partner nations
- Commercial behaviour of suppliers (eg monopolistic providers – cf TSCP)
- Commercial policy and behaviour (particularly for joint working) in MOD
- Only Government departments allowed to buy from CCS/Government Marketplace
- Elements within Government/MOD frustrate collaborative working with industry (arms-length vs co-working on requirements (including joint requirements))

Opportunities to be explored by the project:

- Granular identity management enables new approaches to security/confidentiality
- Engagement with SDA to understand current best practice in high-risk, high-threat environment
- Empower non-Governmental bodies – with bone-fide Defence needs – to purchase from CCS without need for MOD sponsor (qv Commissioning Customer)
- Federate capabilities and standards wherever achievable
- Compartmentalize CWEs around communities and caveats