Cross Domain Secure Mobility service from 2T Security

We design, build and support SECRET mobile systems for accessing classified data and domains, in line with NCSC patterns and our work in Advanced Mobile Solutions (AMS). Cross Domain Gateways (CDGs), ephemeral systems design, tailored monitoring and strict data definition protect sensitive and high threat systems against sophisticated threat actors

2T Security have been working with NCSC on their Advanced Mobile Solutions (AMS) programme of work since 2016. This programme of work has designed security techniques and solutions for solving some of the complex issues that arise with the use of commercial mobile devices in high-threat environments that access sensitive data in a "high side" back-end. These designs are being published as the NCSC's formal guidance on how to implement mobility in a high-threat environment, and 2T Security are responsible for the security design of the AMS architecture on behalf of NCSC.
As a result of this engagement, we are competent to provide a number of service offerings to appropriate clients, including:

1) Consultancy – we can help to solve your mobile challenges using existing technology and patterns, or if appropriate, work with you to design new solutions to problems that have not yet been solved. All with the backdrop of reality through our experience – we will call out if the resultant risk profile of the solution is likely to be too great for the organisation for particular scenarios.
2) Cross Domain experts – we have extensive experience of designing systems to make use of Cross Domain Gateway (CDG) technology, and understand how to mitigate the risk of vulnerability exploit on the "high side" through careful data description and management, coupled with a hardware-based CDG. We have also provided assurance for third party implementations through the review of their architecture, and in particular, data design.
3) AMS Architecture assurance – where standard mobile apps and services need run across a cross domain mobile, we support third parties who create "AMS middleware" that sits between the client and server through design review and assurance, and where appropriate, ongoing support through the development of the project. We have even provided "Product Owner" style support for managing the resultant deliverable.
4) Secure Mobile systems – we design, deploy and support AMS-based systems that can be tailored to specific user requirements, taking operational requirements and risk appetite into account.

All of the above offerings can be tailored to fit your requirements if necessary, and we can liaise with NCSC Security Architects to obtain advice, design review or general opinion based on their privileged knowledge if required.

Operating as an independent organisation, we provide a non-biased vendor-neutral view on problems and their solutions, and will always ensure we remain faithful to our security morals and openly and honestly reflect our professional security opinion; even if this means being the bearer of bad news within a project. Our philosophy is to provide only the amount of help and support that is required; we are happy to teach our clients how to build and run their

solutions to enable in-house management, or we can work autonomously and deliver them an environment that allows them to focus on their core business functions.
If you require support in the technical security space, then we can help. We can support with small or large projects, across a wide variety of security disciplines.

Capabilities

- Custom design and build for tactical sensitive mobile systems.
- Cross-Domain expertise for robust inter-domain segregation.
- Establishing security requirements for the project, including both the business requirement and the security requirement and constraints.
- Designs align with NCSC patterns for Advanced Mobile Solutions (AMS).
- Ephemeral technology used to provide enhanced system security.
- Strong data design and typecasting for effective CDG deployment.
- Support available for individual components or whole mobile ecosystem.
- Experience of safely passing complex crypt/protocols across CDGs.
- We provide non-biased vendor-neutral view on problems and their solutions.
- Tactical or strategic architecture for projects, and migration support.
- Solutions solve complex issues using of commercial mobile devices.
- User journey and process review and support, ensure that the process being developed is “sane” from a security perspective and not susceptible to simple abuse or fraud.
- Security Architecture - tactical and/or strategic architecture for the project, and migration support from an as-is state to the new to-be state.
- Review and security interaction with suppliers including requirements, design and implementation.
- Security support with custom applications, measures to improve the security provenance of the application.

Key benefits

- Confidence your technical security problems will be managed by an NCSC assured organisation.
- Confidence that your security architecture is being delivered to a consistent standard.
- Backed up by extensive real-world experience covering most central Government departments and organisations.
- Modular approach to functionality — we can support and rapidly deliver a minimal set of requirements for a client's immediate needs, which can then be augmented in stages to support enhanced requirements.
- Services led by UKCSC Chartered, ACSC Security Architect, Head Consultant

Engagement Process

Our security architecture service engages widely to deliver high levels of value to your business, including:

- Identifying business, technical, and supplier stakeholders.
- Understanding existing security controls for effectiveness and response capabilities.
- Risk assessments to identify your most critical business assets.
- Developing response plans to protect your controls to protect business assets in the most efficient way.
- Regular checkpoints to review performance and deliver continuous improvement.