MINDLINK

TECHNICAL WHITEPAPER:

MISSION ASSURED FEDERATED REAL-TIME COMMUNICATION

MindLink Engineering

Company
MindLink

Website
mindlinksoft.com

Overview

This whitepaper examines chat messaging communication solutions for seamless mission-wide, multi-domain and multi-classification collaboration in operational National Security and Defense scenarios. We start by establishing the importance of such capabilities across a future coalition mission theatre.

We explore different approaches to achieving a *federated* architecture in a mission context, concluding that a chat room-based "**Persistent Chat"** user experience offers unique advantages in collaboration, discovery, and threat mitigation over alternative paradigms. We expand upon federated Persistent Chat towards achieving a new generation of **assured Persistent Chat,** specifically designed for classified information sharing whilst guarding against the prevalent and sophisticated threats using data-centric and zero-trust principles.

We discuss the challenges in achieving a secure, mission-ready system for exceptionally classified multi-domain operations in a federated network. We then look at how MindLink has overcome these challenges in development of the FRNIX communication protocol and its integration into the data-centric security architecture of the established MindLink platform.

Messaging-based communication paradigms

In the last 20 years, real-time chat messaging has become ubiquitous with consumers, within business, and across National Security and Defense (NS&D), but there are different *forms* of real-time chat messaging that lend themselves to different scenarios. We discuss the benefits of each of these below.

Ad-Hoc Instant Messaging

Perhaps the most prevalent, ad-hoc instant messaging is a conversation between two or more users that is created on-demand and often has a short life span. This is an effective means to quickly “catch-up” or “synchronize” with others.

Participants in an ad-hoc instant messaging conversation are invited directly and once they are out of the conversation can only get back in when another participant invites them.

Once a participant leaves the conversation the content is lost to them.

Scheduled Meetings

In scheduled meetings a future date is set for a conversation, often involving multiple types of communication (modalities – IM, audio, video, screen sharing). Participants are explicitly specified by an organizer and can come and go as needed throughout the meeting.

Once the meeting ends often the content is lost after a grace period.

Persistent Chat Rooms

With chat room-based messaging, a chat room “manager” creates a room that has a *persistent* content history and specifies access control rules for members. A member of a room can come and go as they please and the persisted content history will remain available to them until the room is removed or their membership rights revoked.

Since rooms are created as long-lived entities, structured and discoverable with automatable access control, their ability to enable collaboration across large groups of connected people is invaluable in a mission context. Since each room has a clear access control boundary, they also naturally act as security containers for sensitive content – though in practice assuring a single system to support multiple security levels typically presents significant challenges.

Use of Persistent Chat rooms has longstanding and proven value in the National Security and Defense mission as a communication paradigm – no other tool can facilitate sharing of such volumes of data so reliably to so many participants. However, it is vital that we continue to innovate in the security, networking, and data architectures of such solutions to keep pace with modern threat models and agility needs.

The need for federated communication in NS&D

There is an ever-increasing need to ensure efficient and collaborative exchange of classified information precisely and ubiquitously across the mission landscape. Doing so is vital to achieving decision advantage and expedient action in the face of our ever more advanced and capable enemies.

However, in reality this landscape is a fragmented mix of different groups of participants, all of whom must somehow be connected, at scale, in real-time. We identify several different information-sharing barriers that prevent this from happening:

- International boundaries, where coalition nations must share information but preserve sovereignty.
- Organizational boundaries, where sharing of mixed intelligence disciplines must be carefully managed.
- Forward-deployed infrastructure boundaries, where low-grade networking infrastructure prevents reliable and powerful communication flow.
- Inter-network boundaries at different classification levels (“cross domain”) – where integrity and security of classified information is protected by the principle of air-gapped isolation.

We propose a “federated” architecture to bridge these disjointed components using a mission-wide interconnected information-sharing network to deliver a reliable, secure, and frictionless collaboration capability.

In designing such an architecture, it is vital that we recognize the unique non-functional requirements of classified mission information sharing:

- **Resiliency** – mission execution should continue even when one or more components is disabled.
- **Data sovereignty** – classified information should remain physically and logically under the control of its owning nation/organization
- **Information governance** – Organizations should retain full control of what information is shared with whom under the principles of need-to-know.
- **Source of truth** – there should be an explicit and consistent logical record of information as it is shared between mission participants.
- **Scale** – the system should scale to tens of thousands of participants across hundreds of networked segments
- **Continuity** – collaboration activities and information silos should persist across frequent personnel changes and operational role assignments
- **On-boarding** – new users should be able to use the full capabilities of the system with minimal manual overheads at short notice
- **Discoverability** – information and users should be easily discoverable
- **Automated assurance** – information security should be guaranteed through automated capabilities.
- **DDIL reliability** – users at the operational edge on low-bandwidth links should be able to fully participate.
- **Cross-domain connectivity** – integration with cross-domain solutions to connect mission participants on network partitions at different classifications and trust levels.

We look to technology innovation to deliver a new generation of collaboration solution that addresses these concerns without compromising usability or efficiency.

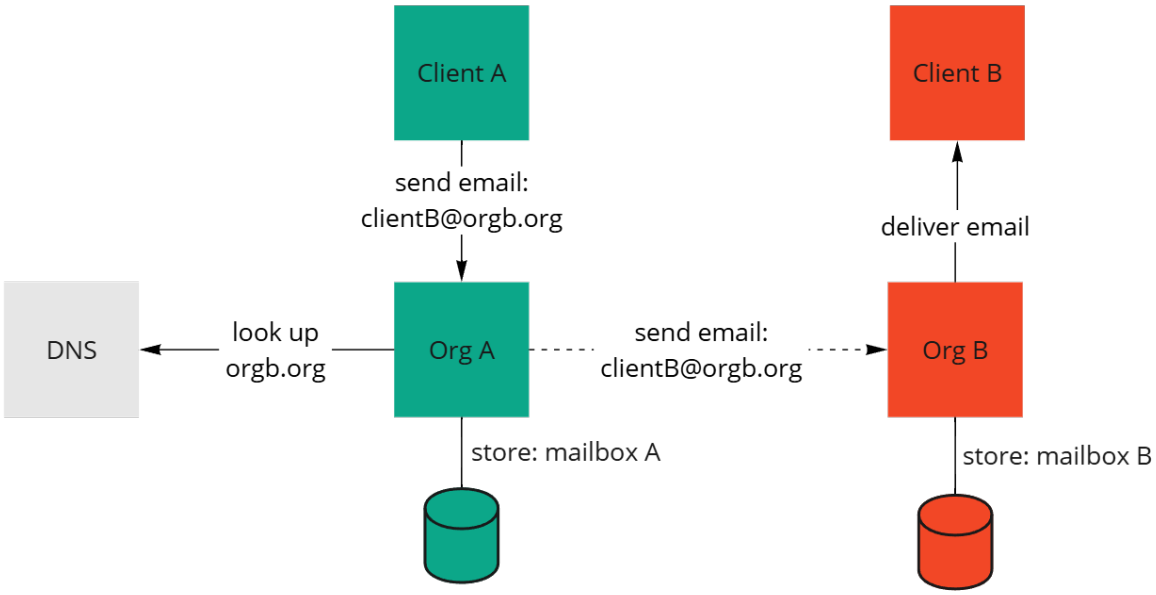
Existing chat messaging-based collaboration solutions

We explore several solution patterns currently deployed for chat messaging-based collaboration (federated and non-federated) in NS&D classified environments.

Email

We start with a brief detour away from the “chat messaging” paradigms previously discussed to email, as it is a prime example of a widely adopted federated text-based information-sharing system.

Email is ubiquitous, frictionless, simple and has stood the test of time.



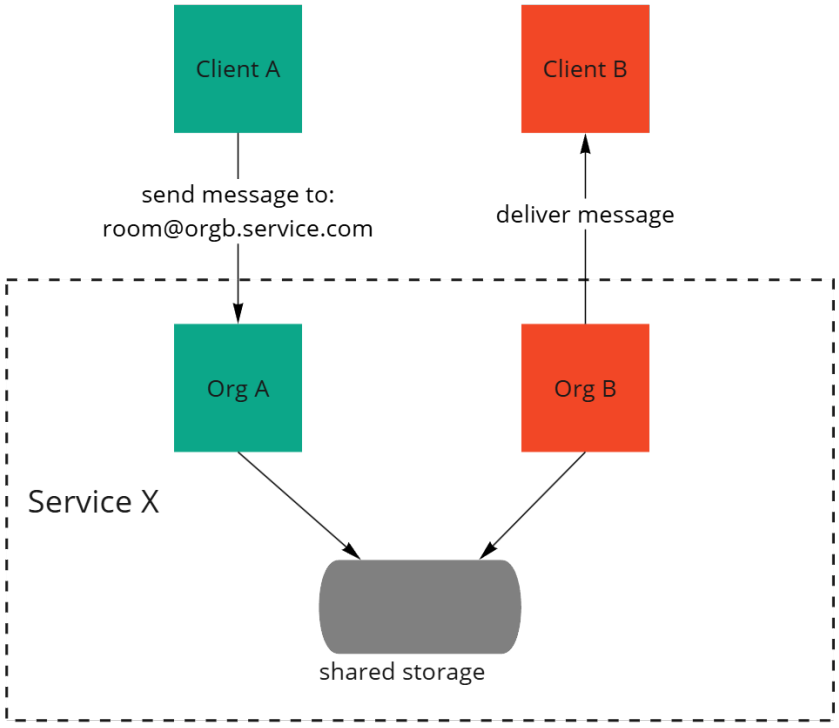
However, the reply and forwarding mechanics of email violate several of our previously stated requirements for classified information sharing:

- **Source of truth**: Within an organization, confidential information ends up fragmented beyond recognition.
- **Information governance** and **Data sovereignty**: Once the information has left your organization you no longer have control over its dissemination.
- **Continuity** and **Discoverability**: Data resides privately within individuals’ inboxes and must be manually reshared with additional/new participants as necessary.

Centralized services

In the commercial space, SaaS chat messaging solutions have had explosive growth over the last decade with the rise of a multitude of offerings from competing solutions providers.

Likewise in NS&D, with a centralized architecture, a service provider (government organization or collaborative working environment “CWE” vendor) hosts secure infrastructure that supports instant messaging and group messaging for multiple organizations simultaneously (multi-tenancy).



Whilst such incumbent systems (including MindLink deployed as a multitenant service) do provide an essential capability to their users and the mission, a centralized approach has several drawbacks according to our aspirational requirements:

- **Data sovereignty:** Chat data resides at rest in the service provider infrastructure (lack of sovereignty).
- **Resiliency:** The centralized service represents a single point of failure in mission-wide operations (lack of resiliency).
- **DDIL reliability:** All organizations and personnel must have reliable connectivity to the centralized service, which limits utility in forward deployed and DDIL environments.
- **Cross-domain connectivity:** The service resides in a particular network and the infrastructure is typically accredited only to a specific classification.

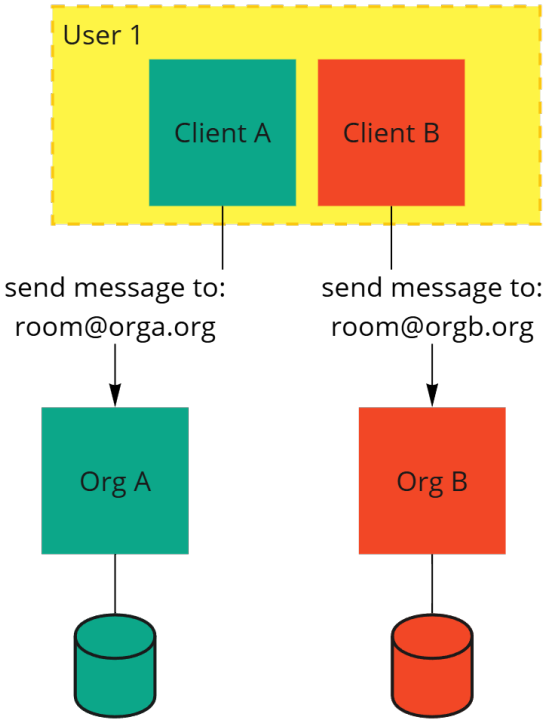
Multi-instance deployment

A multi-instance deployment is where multiple collaboration systems are maintained independently to serve different user estates, organizations, and classification levels, and users log into *each system* depending on their need.

This allows an individual to participate in different mission activities simultaneously whilst doing so with clear boundaries and risk-management behaviors. However, each end user requires multiple client applications – or even endpoint devices – to access each system.

Some hosted solutions essentially operate in this way, requiring users to “log-in” to a specific organization, with the ability to switch organization.

MindLink Anywhere lends itself to this deployment scenario, as its web-based access allows different organizations to expose their internal chat systems to external partners.



However, this approach presents significant challenges to achieving optimal operational effectiveness:

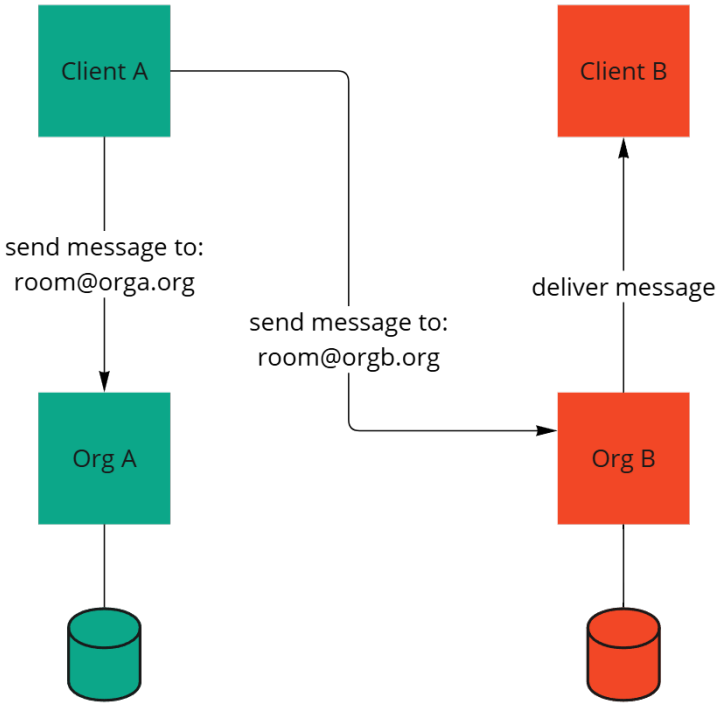
- Users will have different accounts for each chat system to which they connect (account mirroring) leading to:
    - Identity fragmentation and increase cognitive load for the end-user.
    - IT infrastructure and expertise overhead.
    - Licensing complications and increased costs.

- Users have to login to multiple versions of the same product, or different products in order to do their job effectively.
    - Identity fragmentation and increase cognitive load for the end-user.
    - Information fragmentation and increased challenge to discover and find information.

Multiplexed clients

A multiplexed client can connect to multiple backend collaboration systems simultaneously. A user has different credentials for each underlying system but is presented with a unified view of activities across systems.

This approach achieves a streamlined experience to the end user whilst ensuring backend isolation of different classified information as necessary. IRC is perhaps the most well-known solution that relies on the client to connect to multiple different service endpoints.



We note several challenges with such a solution:

- It is difficult to find a client that has enterprise level support.
- Users have different accounts for each chat system to which they connect (account mirroring) leading to:
    - Identity fragmentation and increase cognitive load for the end-user.
    - IT infrastructure and expertise overhead.
    - Licensing complications and increased costs.

Federated Persistent Chat

Federated chat solutions existed long before SaaS solutions and attempted to support the interoperability of email in the context of instant messaging.

Open standards were developed to support such federated capabilities (e.g. XMPP), but these tended to only address instant messaging scenarios between two individuals or ad-hoc conversations between 3 or more individuals (“XMPP multi-user chat”).

The promise of Federated Chat is to allow users in different organizations using distinct chat system infrastructure to participate in conversations together in the same way as conversations within a single organization.

Unfortunately, the technology of 10-20 years go now falls short in providing assured communications in a mission context.

We identify the following gaps in available solutions:

- Assured Federated Persistent Chat for highly regulated scenarios.
- Chat solutions secured against current and future threat models, leveraging contemporary security architectures (e.g. zero trust)
- Chat solutions capable of sharing classified information, compatible with mission infrastructure, and supporting and enabling operational mission workflows.

Towards Federated Persistent Chat

We lay down the foundations of a new generation of federated persistent chat platform for classified mission scenarios. We start by considering fundamental design decisions from first principles.

Chat rooms are persistent and have explicit membership governance, but which organization has control over the access and dissemination of persisted chat data?

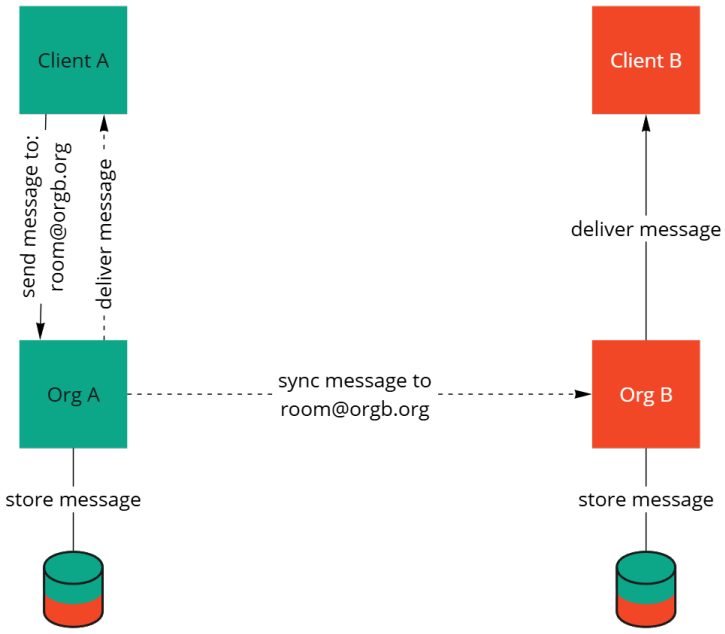
We have identified that there are two types of data architecture for federated chat rooms - the shared ownership and the exclusive ownership models.

Shared Ownership

In the Shared Ownership Model, each participant organization of a chat room simultaneously has full control over their own view of the shared data.

The act of federating a room has the effect of mirroring the content across all federated participant organizations' at-rest infrastructure. Each organization also maintains a view of the membership and oversees enforcing membership constraints themselves.

- Each organization can participate in the chat room even in the face of loss of connectivity – the chat room content is merged across organizations when connectivity is available.
- Each organization has a persistent mirror of the chat room content.
- Each organization authorizes their own users based on a mirrored access control list.
- This is also a suitable model for federation between deployments in the same organization where trust is high, but connectivity may be unstable.



We note that this model critically violates our requirements for classified information sharing in the following ways:

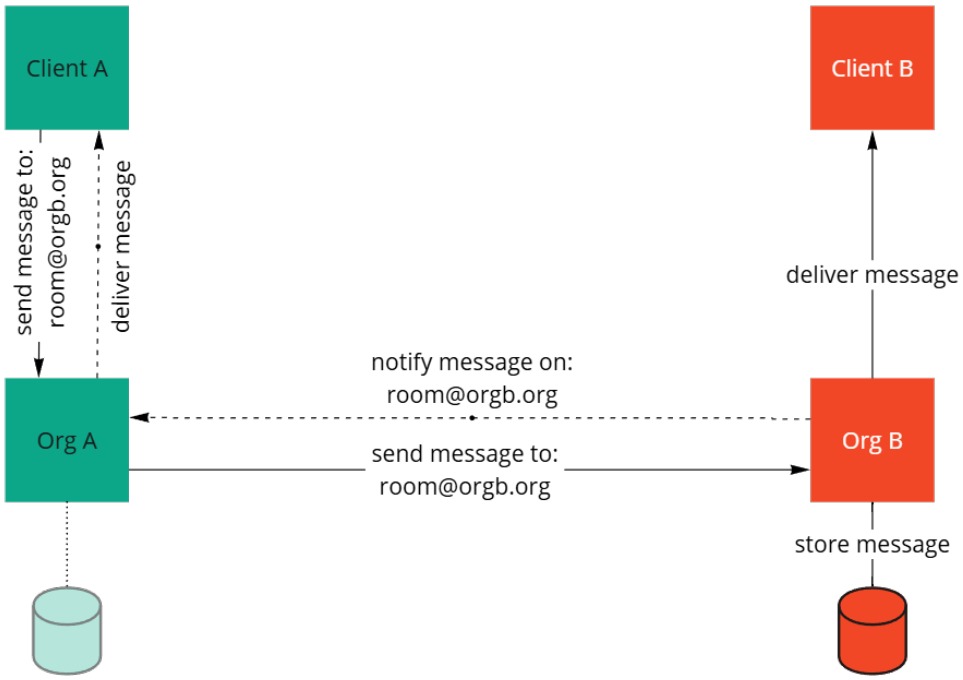
- **Data sovereignty –** Data is stored at rest by all organizations, with no notion of sovereignty
- **Information governance** – Data is shared equally and transitively between all organizations with no notion of explicit governance.
- **Source of truth** – Data is duplicated across all nodes with no delivery guarantees and may become split-brained in the event of network failure.

Exclusive Ownership

In the Exclusive Ownership Model, a single owning organization has control over the data in each chat room.

The act of federating a room has the effect of providing real-time on-demand access to the room content to each federated participant organization. The exclusive owner organization of the chat room makes authorization decisions and forwards those decisions in real-time to the participant organizations.

- Each user in a participant organization can only participate in the chat room if there is connectivity from their organization to the exclusive owning organization.
- Each user in a participant organization has an ephemeral copy of the chat room content for the chat rooms they have joined, persisting the content is a violation of the federation protocol.
- Only the exclusive owner organization has the access control list and makes authorization decisions.
- This is a suitable model for federation when you want persistent chat room content only in the owner organization and you are providing *access* to that content to users in other organizations.



We note that this model satisfies all our requirements for classified information sharing. This approach balances the need to **share** with the needs to **control** and **protect**.

We therefore use this architecture as the basis for a federated capability within MindLink.

Onwards to Mission-Assured Federated Persistent Chat

The MindLink platform has been engineered to enable seamless sharing of classified information, en-masse and at the speed of mission. It embeds intelligence handling practices as first-class principles through cutting-edge cybersecurity techniques such as data-centric security (DCS) and zero-trust (ZT).

In the move to a federated architecture, we are required to extend these information assurance capabilities across a distributed network, securing information as it is shared according to the “need-to-know” between partner nations, organizations, and mission components.

To this end, MindLink worked with the UK Defence and Security Accelerator and FVEYs SIGINT community to develop the FRNIX (“Federated Real-time Need-to-Know Information eXchange”) protocol to enable classified information to be shared in persistent chat rooms between federated partners.

FRNIX handles negotiation and transmission of assurance metadata to enable MindLink security capabilities to be enforced across mission information-sharing boundaries:

- Data labelling – human and machine-level representation of DCS attributes for all data, including classification and other multi-layered properties.
- User entitlements – resolution of user security attributes and other metadata for ABAC control decisions across federated ecosystem.
- Data Leakage Prevention (DLP) – enforcement of DLP controls across all federated components according to policy set by owning organization.

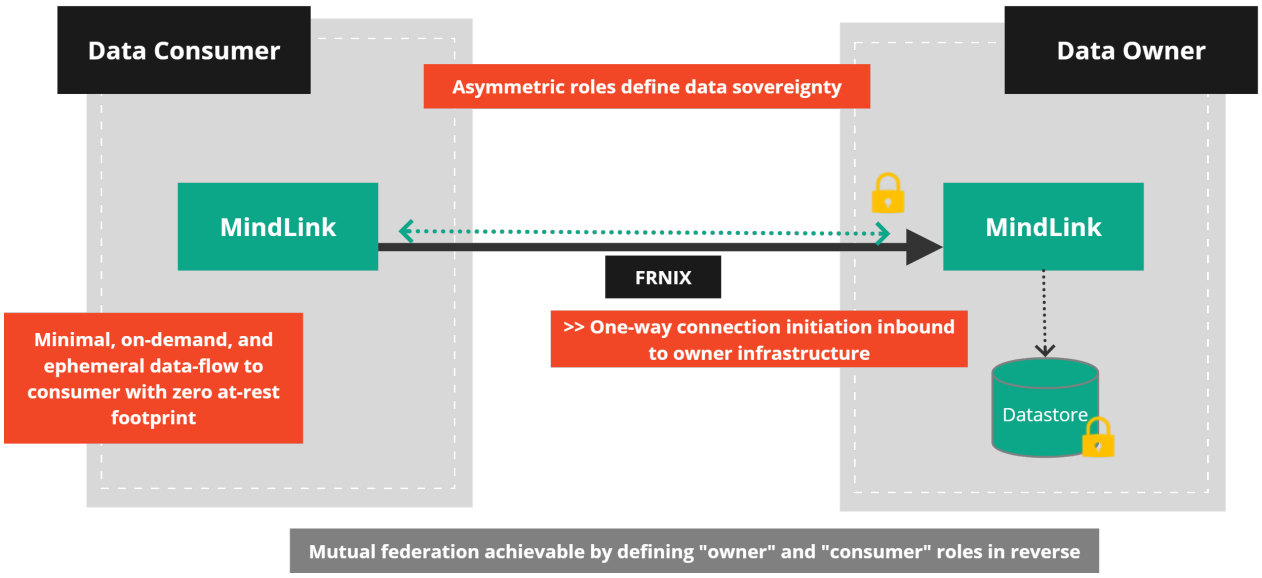
The design of FRNIX has been specifically engineered to mission security and operational requirements to deliver a best-in-breed solution for security, connectivity, and user experience. A MindLink deployment federated over FRNIX exemplifies zero-trust data-centric patterns for information sharing as described in NIST SP 800-207 and NATO ACP-240.

FRNIX: Data architecture

FRNIX explicitly models the “exclusive ownership” data architecture through an asymmetric design. Any two servers communicating over FRNIX each take on a role of “owner” or “consumer” for a chat room, its access control rules, and its content – this enforces the **data sovereignty** requirement.

Such asymmetry extends to the network architecture – connections are initiated one-way from consumer to owner, eliminating inbound network exposure of participating organizations unless they explicitly opt in to sharing their own information.

Data resides at rest in in the “owner” organization’s MindLink infrastructure and is shared ephemerally to each “consumer” where it is cached in memory for a limited period. This minimizes surfaces and lifecycles for data loss and enhances the “**information governance**” requirement.



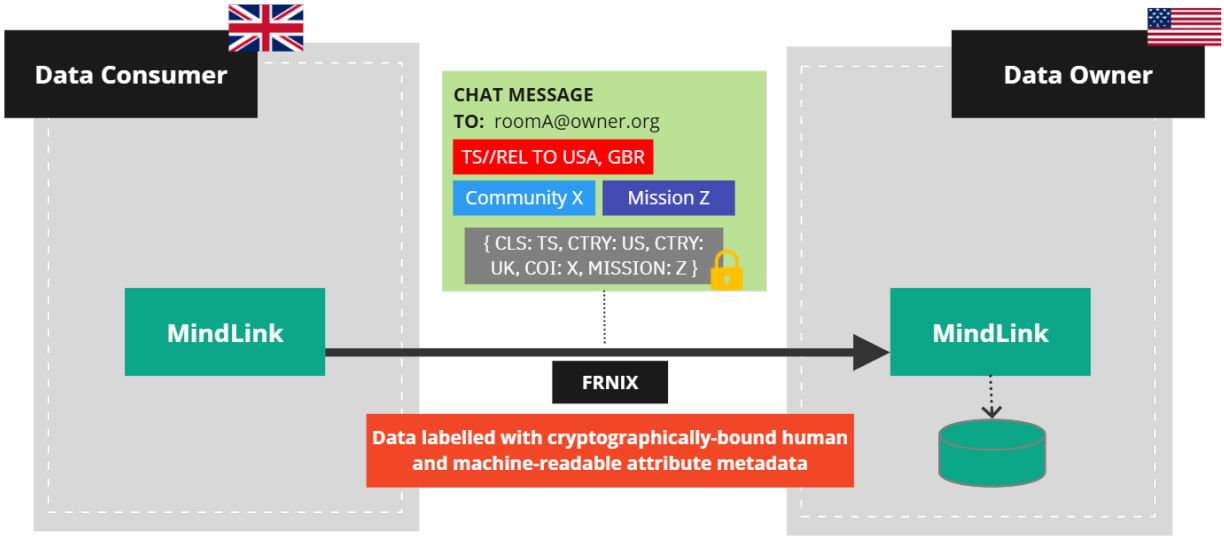
FRNIX: Data labelling

Annotation of data with semantic and security attributes is fundamental to the emerging practice of “data-centric security”. In turn, this approach enables the move away from network-centric security architectures to that of “zero-trust”.

The MindLink platform has embraced data-centric labelling as a first-class principle. Data labels are applied to all content from a hierarchy of controls, including government classification labelling standards, as both human and machine-readable constructs.

The FRNIX protocol transmits these data labels between federated partners as cryptographically bound metadata around classified information packets. This enables multi-classification operations to be delivered over the same infrastructure, with granular, pervasive and distributed enforcement of access-control and handling logic as data is shared across the mission landscape.

Data labels are defined using customizable schema-based configuration. The multi-layered architecture is designed to support the complexity of attribute control-sets and classification labelling typically applied in US, FVEYs, and NATO environments.



Data labelling forms the foundations of further assurance capabilities and enables the FRNIX network to maintain **information governance** on behalf of the owning enterprise. It also underpins delivery of the **discoverability** and **automated assurance** requirements, as described in the next section.

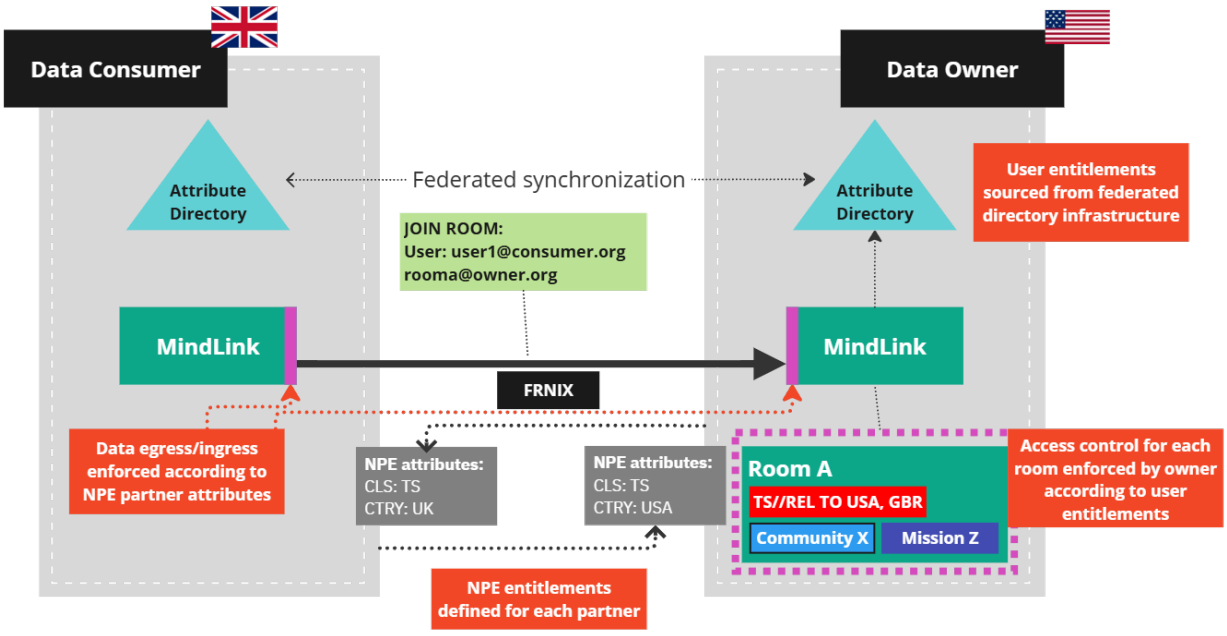
FRNIX: Attribute-based access control

Corollary to data-labelling is the concept of attribute-based access control, where user and service entities are assigned entitlement attributes defining multiple aspects of their clearances, trust and risk profiles. These attributes are then used to make access-control decisions on attribute-labelled data according to multiple layers of attribute intersection logic.

The MindLink platform evaluates all chat room access control decisions in terms of automated ABAC and is optimized to do so at scale and in real-time. The FRNIX protocol enables these such decisions to be made in a federated context, satisfying our **scale** requirement and the need for **automated assurance**.

FRNIX coordinates the resolution of entitlement attributes for federated users between federating partners. It automatically negotiates registration of new users – and evaluation of resulting room ABAC rights – delivering our **discoverability** and **on-boarding** requirements.

Further, FRNIX models service-level data flow across the FRNIX network in terms of attribute-based security, using non-person-entity attributes to authorize backend server operations and data transmission between federating nodes in real-time. This provides full control of both user and service activity using a unified data-labelling and access control schema: distributed **information governance.**



FRNIX: Data leakage prevention

The MindLink platform protects classified data using a “defence in depth” approach. Multiple controls and protections are assigned to both backend processes and the end user interface to prevent accidental or nefarious information leakage.

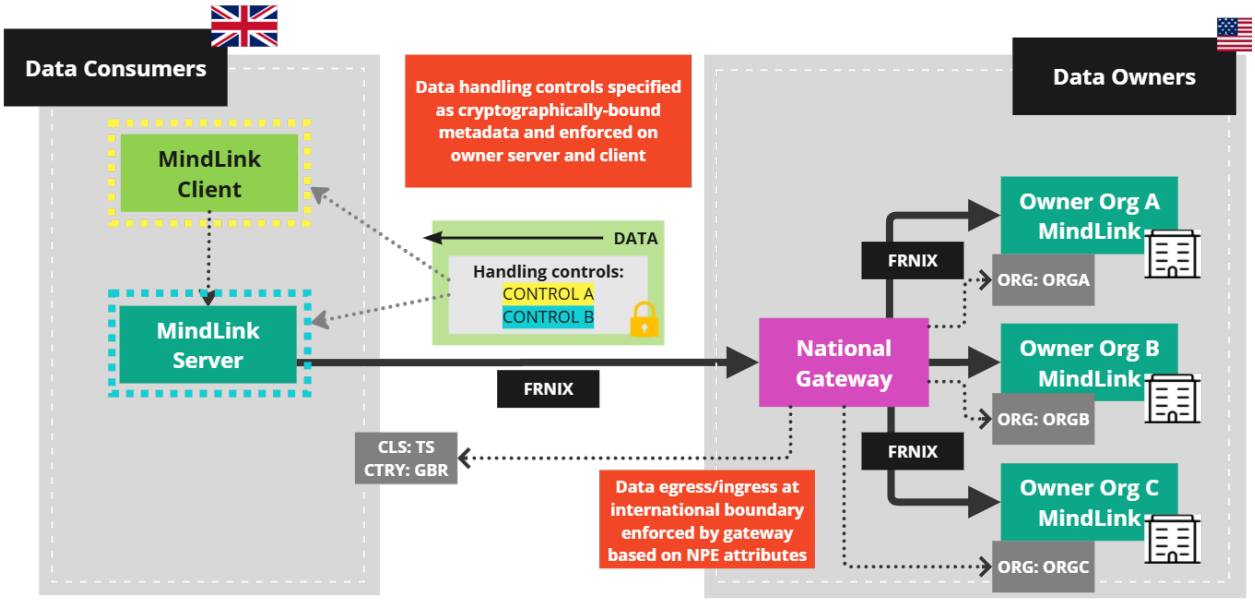
With FRNIX, this capability is extended twofold:

- End-user DLP controls (e.g. copy-paste protection) are flowed to federated users’ clients and enforced per-room according to policy defined by the sovereign owner. This provides **data sovereignty** and **information governance.**

- FRNIX connections are routable through intermediary gateway tiers as necessary by the network or security architectures. Such gateway components are able to inspect, verify, and enforce onward data transmission according to the cryptographically bound data attributes on each protocol message.

  For instance, a country may deploy a national FRNIX gateway to handle all traffic from its internal agencies exiting the international boundary. The gateway can enforce that traffic is releasable to its onward destination, providing additional layers of **information governance** through **automated assurance**.

FRNIX’s data-centric architecture allows data to be continuously supervised and protected as it flows across the federated mission network.

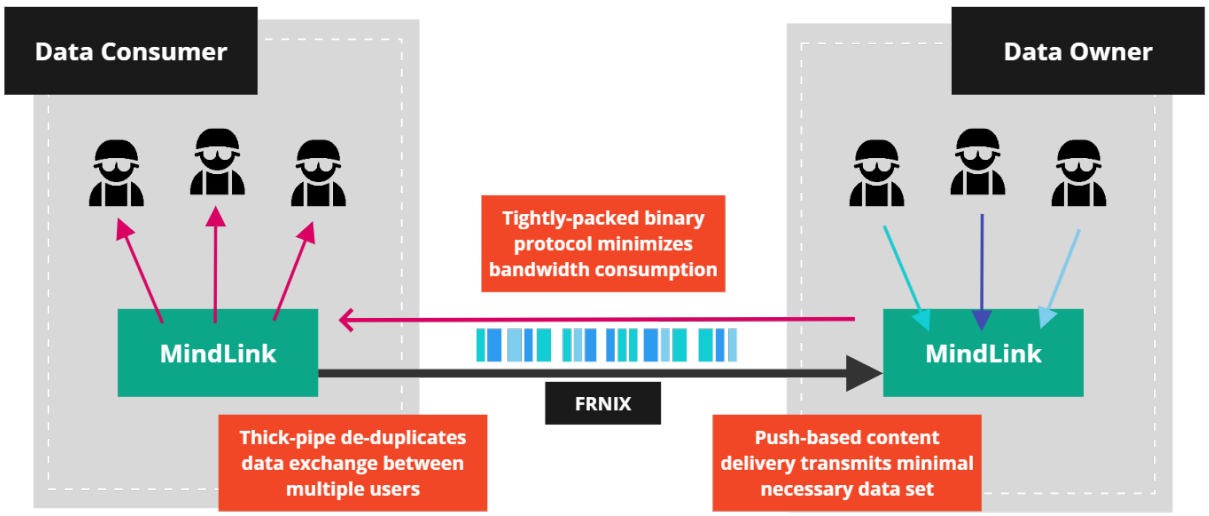


FRNIX: Low-bandwidth connectivity

The MindLink platform is proven in delivering vital intelligence sharing to those working in forward-deployed positions on land, sea, and air. The client-server protocol has been tested and used in action over low-bandwidth radio and satellite network links.

The transition to a federated architecture enhances the **resiliency** of such a solution – groups of users deployed at the tactical edge may continue to collaborate across wider communication outages. FRNIX has been engineered as a federation protocol to operate reliably and efficiently over low-bandwidth connections (**DDIL reliability**):

- The protocol leverages highly compressed data streams for transmission, minimizing bandwidth profile.
- The protocol is event-based using a fan-out architecture, minimizing traffic sent over the federated links.
- Reconnect and retry semantics are embedded into the protocol, ensuring reliable and efficient recovery.
- Network and node liveness are explicitly modelled in the protocol - this enables recovery but also ensures that end users are fully informed as to the real-time status of information availability and dissemination.



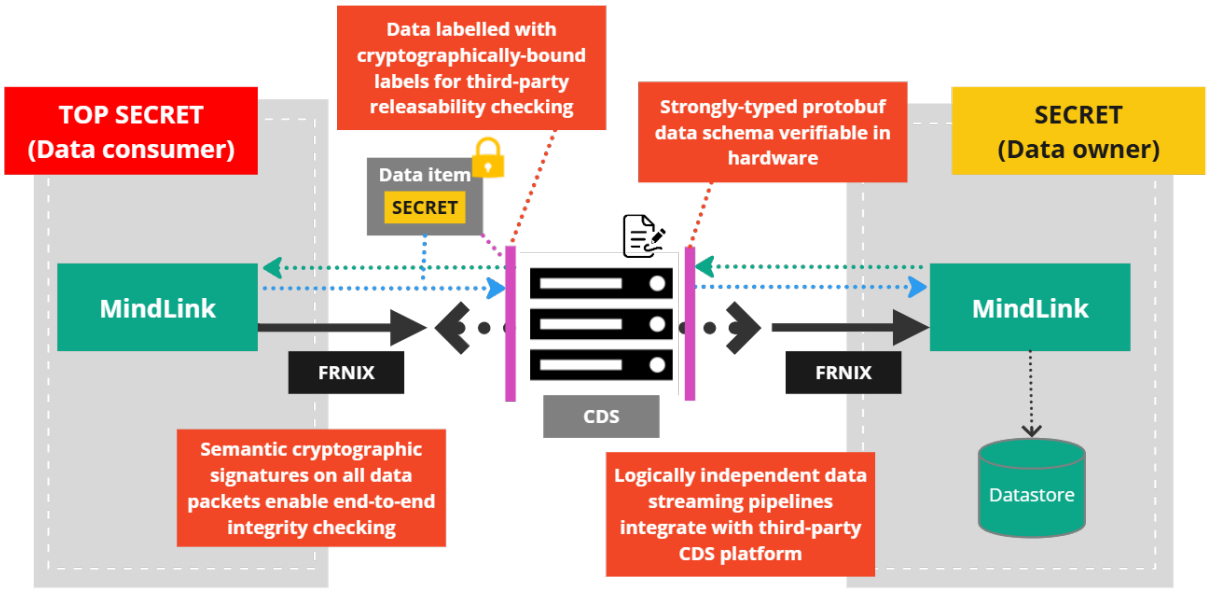
FRNIX: Cross-domain collaboration

Achieving seamless mission-wide information sharing requires connecting those working on physically isolated networks, often at different classification levels: **cross-domain connectivity**. Delivering a fully integrated user experience and federated architecture requires moving data between networks using highly assured third-party “cross domain solution” (CDS) infrastructure.

Given the levels of validation and verification that a CDS must perform, they typically offer a highly restricted and API channel over which to send or receive network to cross-domain counterparts. As such, achieving end-to-end connectivity over a CDS is a complex engineering challenge – with different integration architecture and throughput characteristics to a standard IP gateway or firewall.

FRNIX has been designed with the restrictions of modern CDS products in mind. The key motivation has been to reduce the complexity of such an integration, whilst maximizing the throughput and assurance offered by the end-to-end solution through various protocol design decisions:

- The overall data architecture explicitly models asymmetrical trust between federated partners.
- The protocol operates over independent unidirectional data streams that can be pipelined over typical hardware.
- The protocol data types are described using static schemas that can be used to generate hardware verification tools embedded as part of the CDS pipeline.
- Data attributes are bound to all content types using cryptographic constructs to enforce end-to-end data integrity and release semantics.
- Such digital signatures are constructed independent of the serialized data, such that verification may be performed around the content disarm and reconstruction processes of the CDS.



In NS&D, CDS solutions must be accredited to an increasingly high national standard – e.g. NCDSMO RTB in the US government. FRNIX has been purpose designed to support such technical requirements roadmaps to build elegant and certifiable end-to-end solutions for **cross-domain connectivity**.

Summary

MindLink's federated capability, underpinned by the new FRNIX federation protocol, delivers a new generation of collaborative information sharing across the complex landscape of the mission theatre. FRNIX has been designed to directly address the core challenges of mission information sharing and is engineered for integration into federated mission network infrastructures using data-centricity and zero-trust as first-class principles.

MindLink and the FRNIX protocol resolve the unique requirements of secure information sharing in the future mission:

- **Resiliency** – a federated architecture mitigates mission execution against the disabling of any given partner.
- **Data sovereignty** – classified information is held physically at rest and logically governed under the control of its owning nation/organization.
- **Information governance** – each organization retains full control of what information is shared with whom under the principles of need-to-know.
- **Source of truth** – there is an explicit and consistent logical record of information as it is shared between mission participants.
- **Scale** – the system scales to tens of thousands of participants across hundreds of networked segments, leveraging the MindLink platform, FRNIX optimizations, and automated ABAC.
- **Continuity** – Automated ABAC allows collaboration activities and information silos to persist across frequent personnel changes and operational role assignments
- **On-boarding** – Automated ABAC enables new users to be onboarded and able to use the full capabilities of the system with minimal manual overheads at day-zero.
- **Discoverability** – Data-centric labelling means information and users should be easily discoverable
- **Automated assurance** – Data-centric labelling and zero-trust means information security should be guaranteed through automated and pervasive capabilities.
- **DDIL reliability** – FRNIX protocol transport and data architecture are designed for low-bandwidth and unreliable networks meaning users at the operational are able to fully and reliably participate.
- **Cross-domain connectivity** – FRNIX protocol is designed to integrate elegantly with cross-domain solutions to connect mission participants on network partitions at different classifications and trust levels to full accreditation.

Funded by the Defence and Security Accelerator, this work presents a step-change capability for both user-experience and security posture of real-time mission collaboration, in full compliance with NIST SP 800-207 and NATO ACP-240. To find out more, please email info@mindlinksoft.com

Appendix – FRNIX: Technical objectives

FRNIX has been engineered to meet the following technical objectives:

AREA	OBJECTIVE	DESIGN RESPONSE
Data sovereignty	Ensure sovereignty and governance of all data is clearly defined	Asymmetric federated protocol defines roles of data “owner” and “consumer”.
	Maintain control of sovereign data, including revocation.	Data physically resides at rest in owner infrastructure only, minimum and ephemeral data flow to consumer parties.
	Single source of truth	Explicit record of ordered message delivery for each conversation, owned by single physical authority
Performance	Minimize network exposure	Single-port communication initiated asymmetrically one-way from consumer to owner minimizes exposed network ingress.
	Support reliable, en-masse real-time collaboration	Multiplexed protocol enables efficient fanout, caching and retry.
	Operate over poor network links	Efficient gRPC streaming transport minimizes network data and connection overheads.
Data security	Leverage corporate authentication and identity	Server trust established using mutual PKI and user authentication driven by corporate directories.
	Enforce strong access control to rooms	ABAC clearances and identity properties resolved for each user from federated ABAC ecosystem.
	Protect classified data	MCE classification system models data sensitivity and releasability to remote partners, including ACL and labelling to government standards.
	Enable multi-classification architectures	All protocol data labelled with cryptographically-bound data attributes using data-centric-security principles.
	Sandbox federated access	Multi-layered MCE security engine segregates federated rooms into walled contexts with associated security controls.
	Encrypt data across all infrastructure components	Network links secured with TLS 1.3 and compatible with MCE at-rest SQL encryption.
	Mitigate insider-threat attack surfaces	Zero-trust architecture by integrating with MCE COI-based end-to-end encryption (phase 2 goal).
Operations	Uphold organizational authority	Trust and identity model based on centralized organizational boundaries and infrastructure.
	Facilitate rapid on-boarding and agile cross-mission operations	Organizational trust and role-based ABAC enable efficient administration across wide and dynamic collaborating population.
CDS Integration	Integrate elegantly with pipelined data-diode hardware	Asynchronous event streaming with decoupled request/response routing over independently established connections
	Enable static hardware data validation	Protocol defined with strongly-typed protobuf schema. Chat messages defined with strict structured data types.
	Enforce release semantics	Data attributes cryptographically bound to protocol messages to enforce releasability and sensitivity of cross-domain traffic via third-party components
	Decouple cryptographic signatures from serialization	Cryptographic signatures calculated over primitive data types enabling content integrity validation even after data transformation and reconstruction.
	Achieve and future-proof accreditation posture	Protocol architecture to uphold US NCDSMO RTB and UK NCSC import/export guidelines and roadmap