MINDLINK

TECHNICAL WHITEPAPER:

SECURE FEDERATED COMMUNICATION

MindLink Engineering

Company
MindLink Software Ltd.

Website
mindlinksoft.com

Overview

In this whitepaper we will briefly examine different communication paradigms and focus on the need for cross-organization communication, *federation*, in a modern workplace.

We will explore different approaches to federated communication and how a **federated Persistent Chat solution** offers unique advantages over the alternatives.

We will expand upon federated Persistent Chat towards **secure federated Persistent Chat** and highlight the challenges in achieving a secure, mission-ready system for exceptionally classified operation and how MindLink is positioned to overcome those challenges.

Communication paradigms

Real-time messaging has become ubiquitous with consumers and within business, but there are different *forms* of real-time messaging that lend themselves to different scenarios.

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.

Group Messaging

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

Often group messaging takes its user experience from Ad-Hoc Instant Messaging, demonstrating a conversational user experience.

Persistent Chat
As a special mention, Persistent Chat is a take on Group Messaging that focuses on mission-optimized usability that both enables and enhances frictionless collaboration over and above traditional tools.

The need for federated communication

People have a need to effectively collaborate across organizational boundaries to deliver value cooperatively, negotiate interactively or effectively contribute to missions that require the expertise of individuals in multiple organizations.

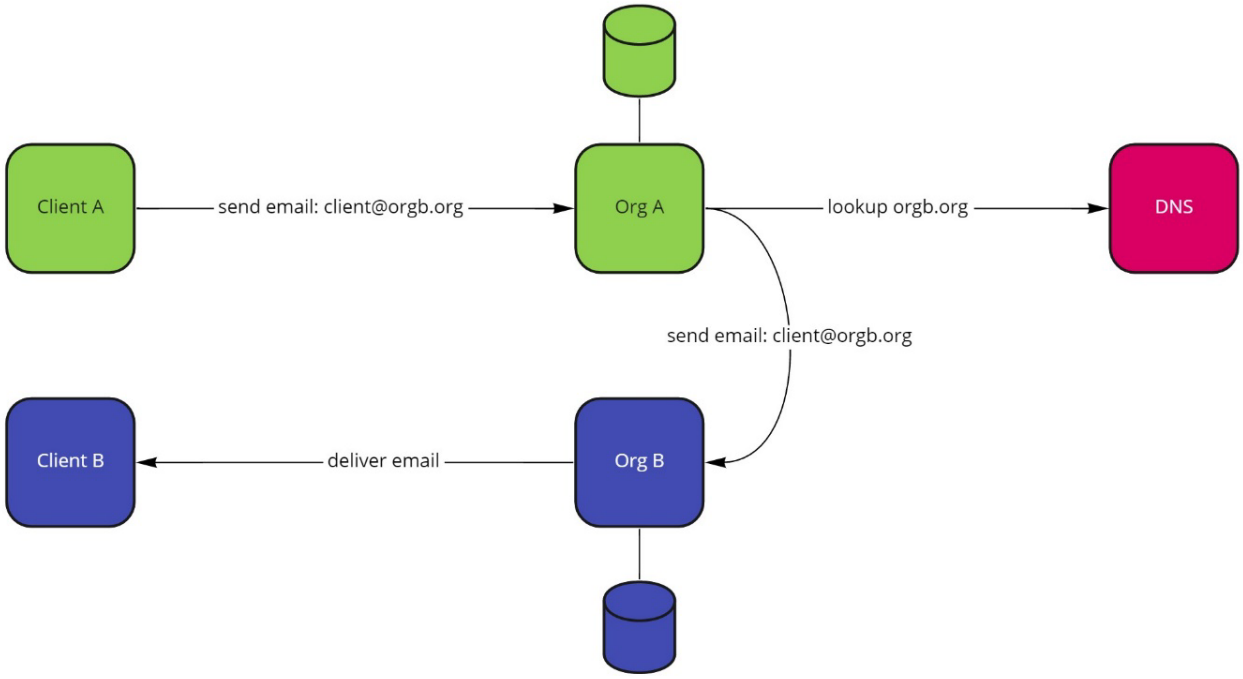
Federated communication is the set of technologies that enable communication across organizational boundaries while allowing an organization to retain sovereignty of their data and chosen platforms.

A secure and valuable federated communication network enables a ubiquitous and frictionless way for people to effectively collaborate across organizational boundaries without losing data protection or control over the dissemination of information.

Existing solutions

Email

Federation is at the heart of the most widely used communication system in the world – Email. Email is ubiquitous, frictionless, simple and has stood the test of time.



The reply and forwarding mechanics of email also raise security concerns:

- Within an organization, confidential information ends up fragmented beyond recognition.
- Once the information has left your organization you no longer have control over its dissemination.

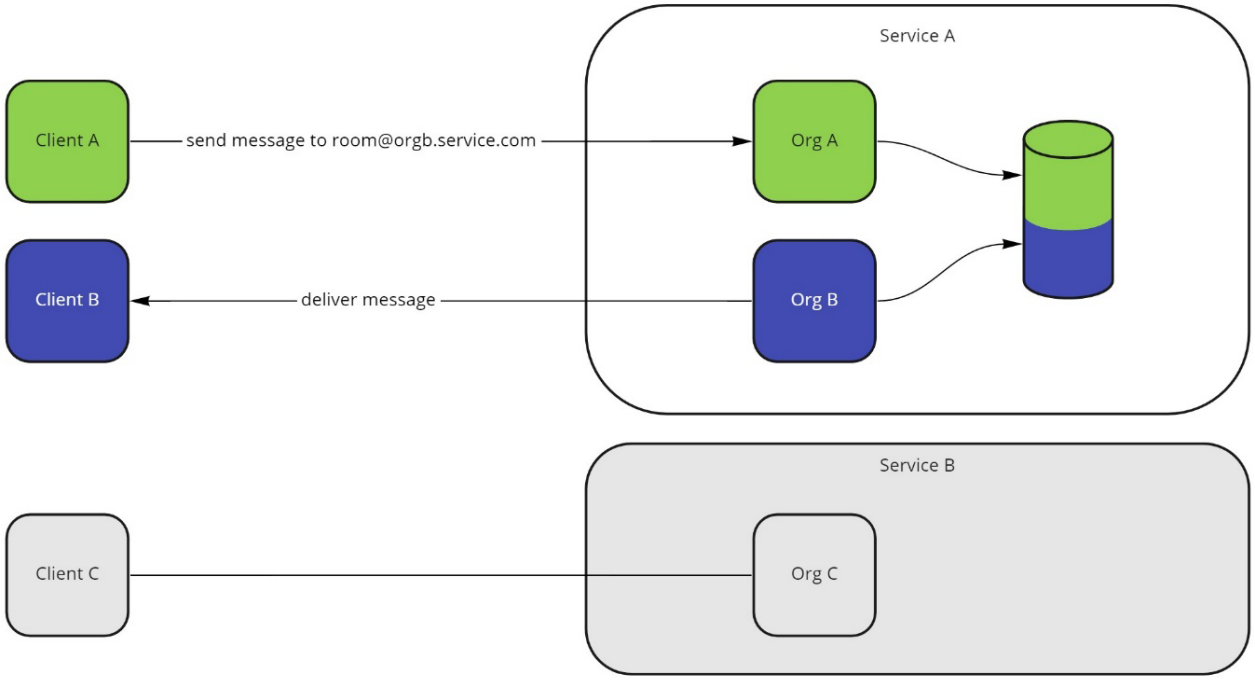
Problems

- Replies and forwards lead to branching conversations that are hard to track.
- Dissemination of information is out of the control of the sender once it leaves their organization boundary (sometimes even within the organization).

Hosted Chat

Hosted Chat has had explosive growth over the last decade with the rise of a multitude of offerings from competing solutions providers.

With Hosted Chat, a service provider hosts infrastructure that supports instant messaging and group messaging for multiple organizations simultaneously (multi-tenancy).



Problems

- If two organizations are using different chat solutions, then they are unable to communicate.
- Chat data resides in the service provider infrastructure.

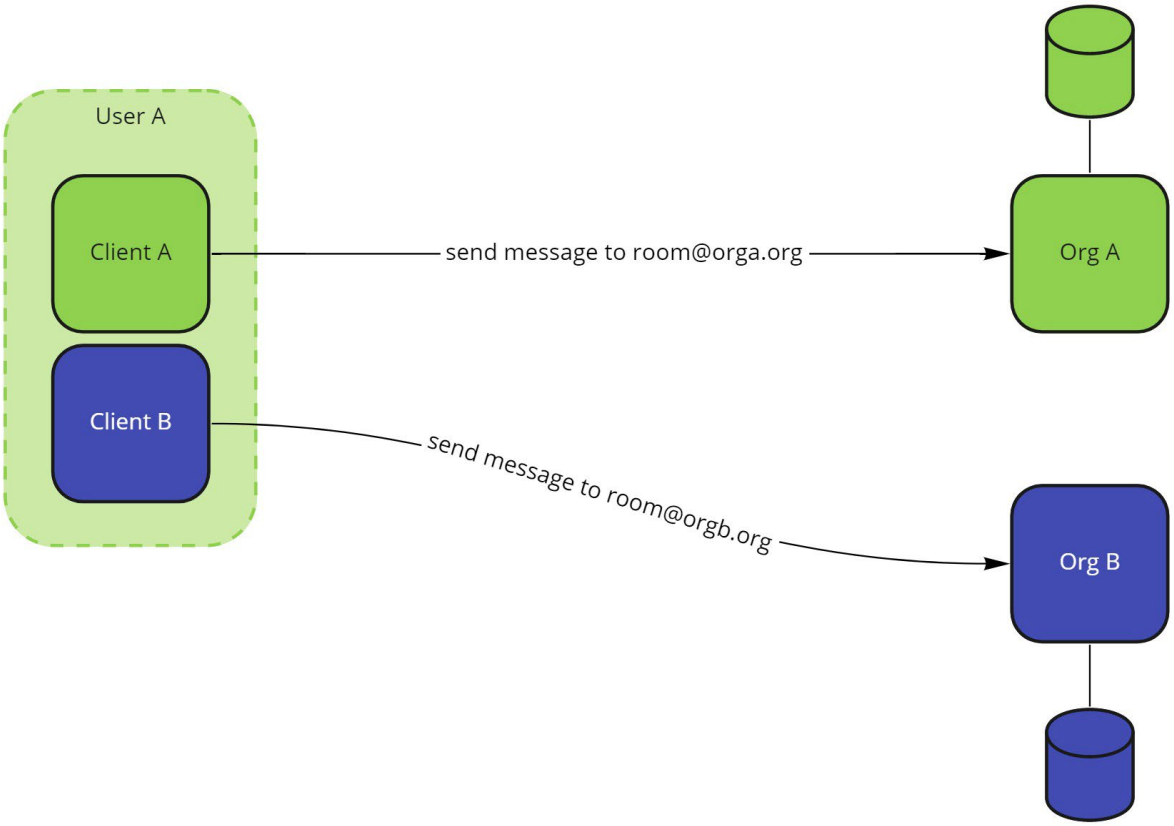
Multi-instance deployment

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

This allows an individual to participate in multiple chat systems with clear boundaries. This can make it clear to end-users which system they are communicating within but needs multiple client applications for the end-user.

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.



Problems

- 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.

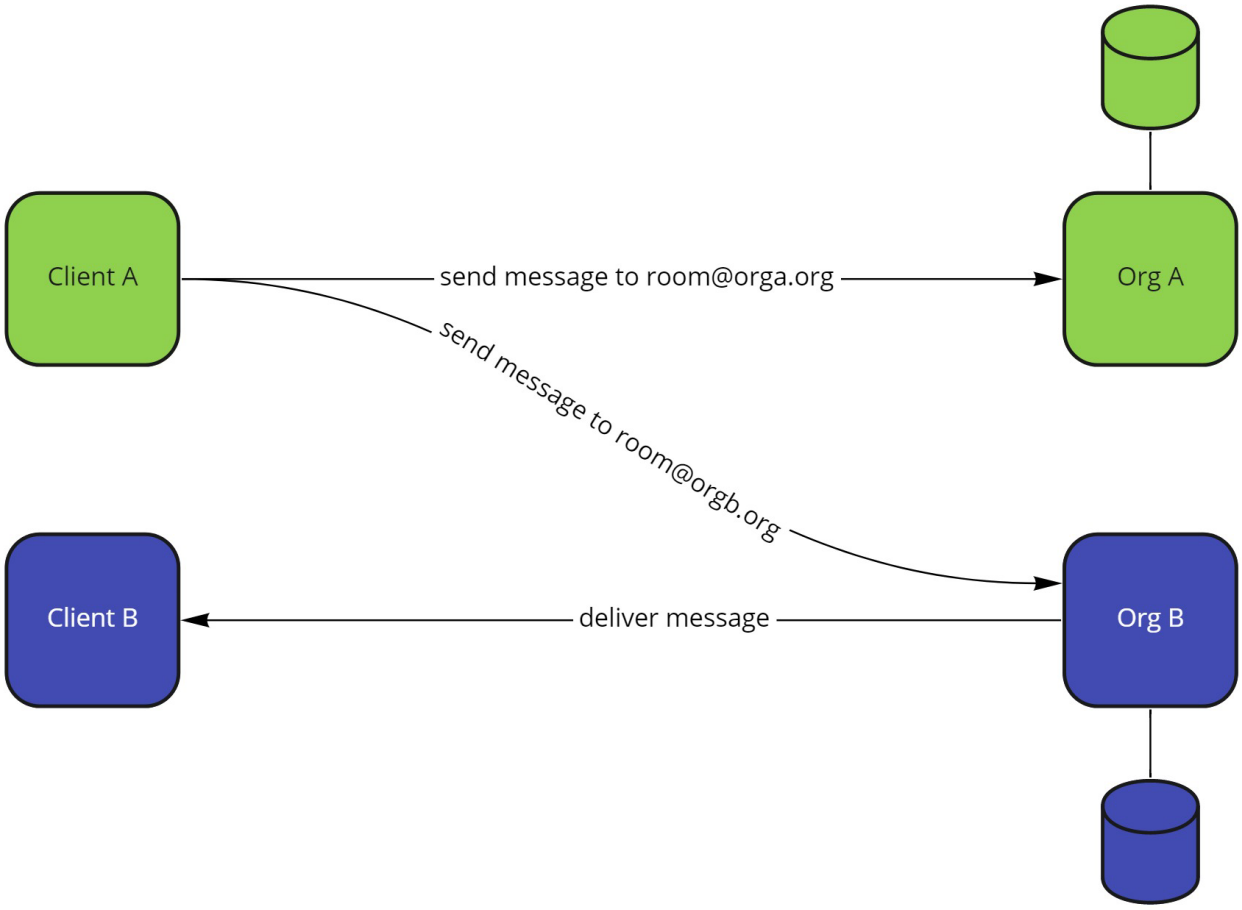
- Users have to login to multiple versions of the same product, or different products in order to do their job effectively.
    - Identity fragmentation and increase cognitive load for the end-user.
    - Information fragmentation and increased challenge to discover and find information.

Multiplexed clients

A multiplexed client can connect to multiple chat systems simultaneously. A user has different credentials for each chat system and is presented with a unified view of conversations across all chat systems.

This allows an individual to participate in multiple chat systems at the same time in a unified experience, but they need to have accounts in each system. Any user wishing for a streamlined experience requires them to use a multiplexed client.

IRC is perhaps the most well-known solution that relies on the client to connect to multiple different service endpoints.



Problems

- 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 Hosted Chat solutions and attempted to support the interoperability of email in the context of instant messaging.

Open standards were developed to support such Federated Chat solutions (XMPP), but these tended to only address instant messaging scenarios between two individuals or ad-hoc conversations between 3 or more individuals.

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

Unfortunately, existing Federated Chat solutions have fallen short in providing a secure and interoperable federated environment.

Problems

- Enterprise-grade Federated Persistent Chat does not exist.
- Exceptionally classified, mission-critical federated solutions do not exist.

Towards Federated Persistent Chat

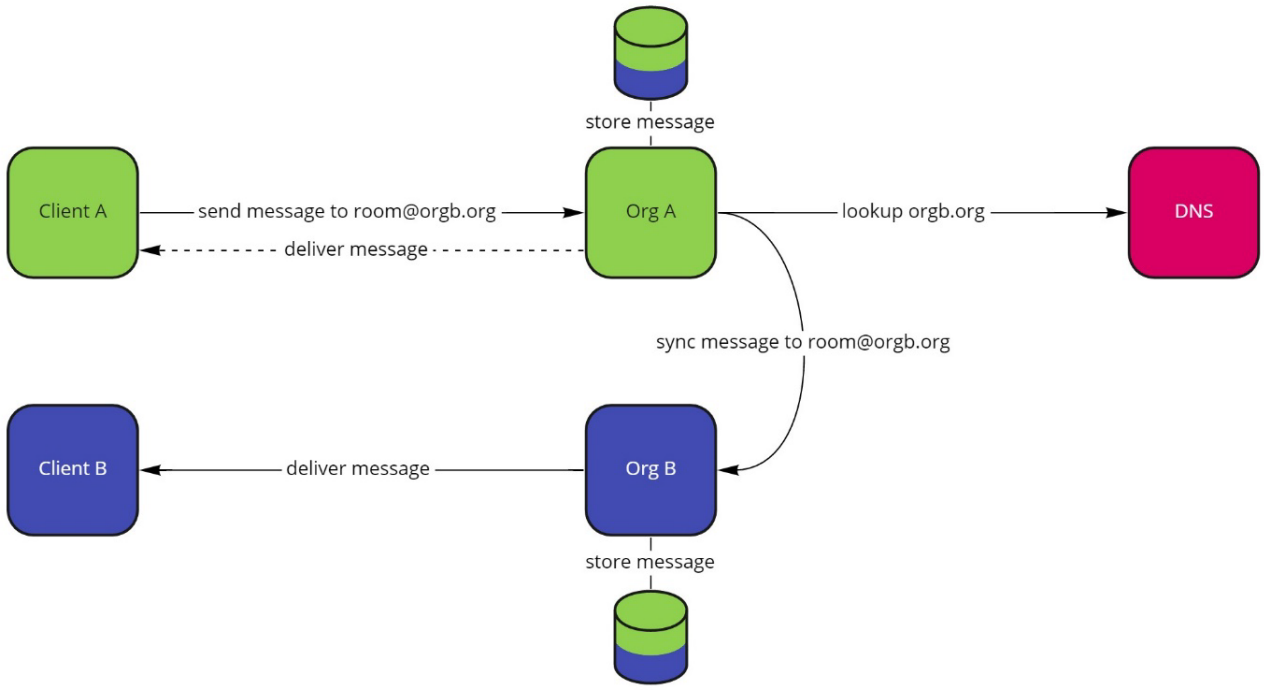
Organizations have differing opinions on what federation looks like in a chat room context. Chat rooms are persistent and have explicit membership governance, but which organization has control over access and dissemination of persisted chat data?

We have identified that there are two types of federation - the shared ownership and the exclusive ownership models.

Shared Ownership

In the Shared Ownership Model, each participant organization has full control over their view of the data. The act of federating a chat room has the effect of mirroring the chat room content across all federated participant organizations, each organization also maintains a view of the membership and oversees enforcing membership constraints themselves.

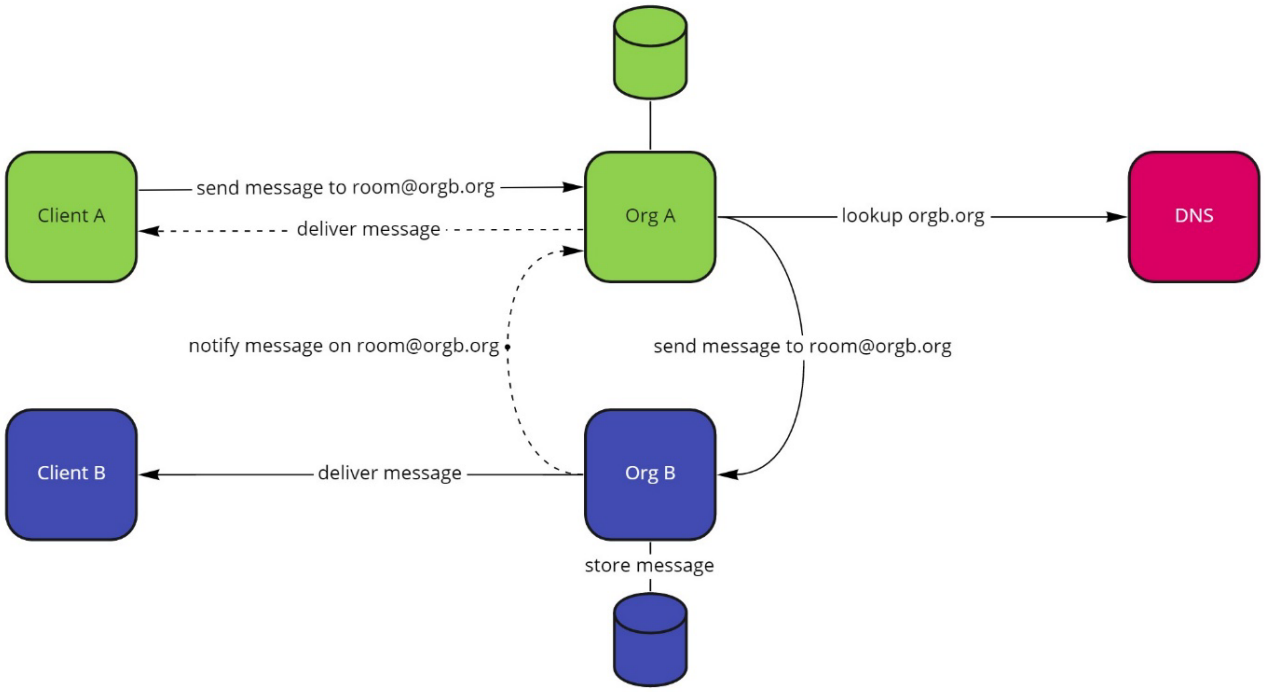
- Each organization can participate in the chat room even in the face of loss of connectivity, the chat room content is merged across organizations when connectivity is available.
- Each organization has a persistent mirror of the chat room content.
- Each organization authorizes their own users based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



Exclusive Ownership

In the Exclusive Ownership Model, a single owning organization has control over the data. The act of federating a chat room has the effect of providing real-time access to the chat 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.



Onwards to Secure Federated Persistent Chat

In addition to basic federation scenarios, there are complex issues that need to be resolved in 4 key areas to achieve a mission-ready system for exceptionally classified operation:

- Classification - sensitivity and dissemination of classified materials.
- Entitlements - authorizing and validating federated identity.
- Encryption - sharing encryption keys across federated organizations.
- Data Leakage Prevention (DLP) – preventing specific sensitive information from leaving an organization.

These key areas are unique to a secure environment where collaboration is required on subjects and information that is exceptionally classified and sensitive. In such environments, heightened protections around the sharing of information are necessary while trying to maintain ease of operation so that information is *implicitly* and *obviously* protected without significant conscious effort from users.

Without implicit and obvious protection, users spend valuable effort ensuring that they are meeting organizational security policy instead of providing value, there is greater room for mistakes and more opportunities for data spillage.

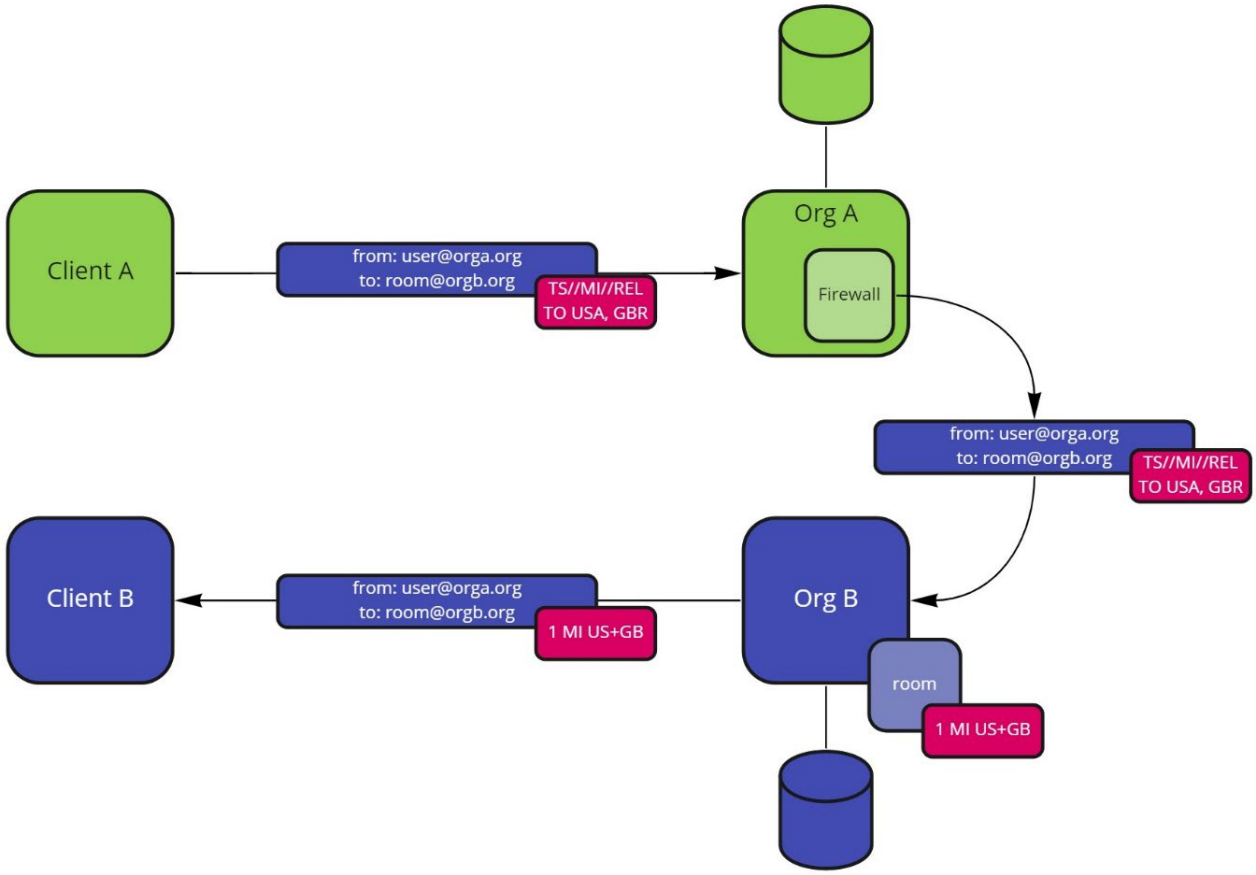
Classification

A “classification” encodes data sensitivity and dissemination controls in a human readable and machine-readable label. A classification is then attached to information. The human readable portion of the classification label is displayed to users so that they are aware of who the associated information can be viewed and shared with. The machine-readable portion enables automatic access control decisions to be made based upon an individual user’s security attributes.

Classified information is labelled with a classification as it flows into and out of organizations. Tools and processes are in place to ensure that only people with the required clearance can read the information. At organizational boundaries, keeping sensitive information from disseminating to individuals who should not have access to the information is a difficult problem.

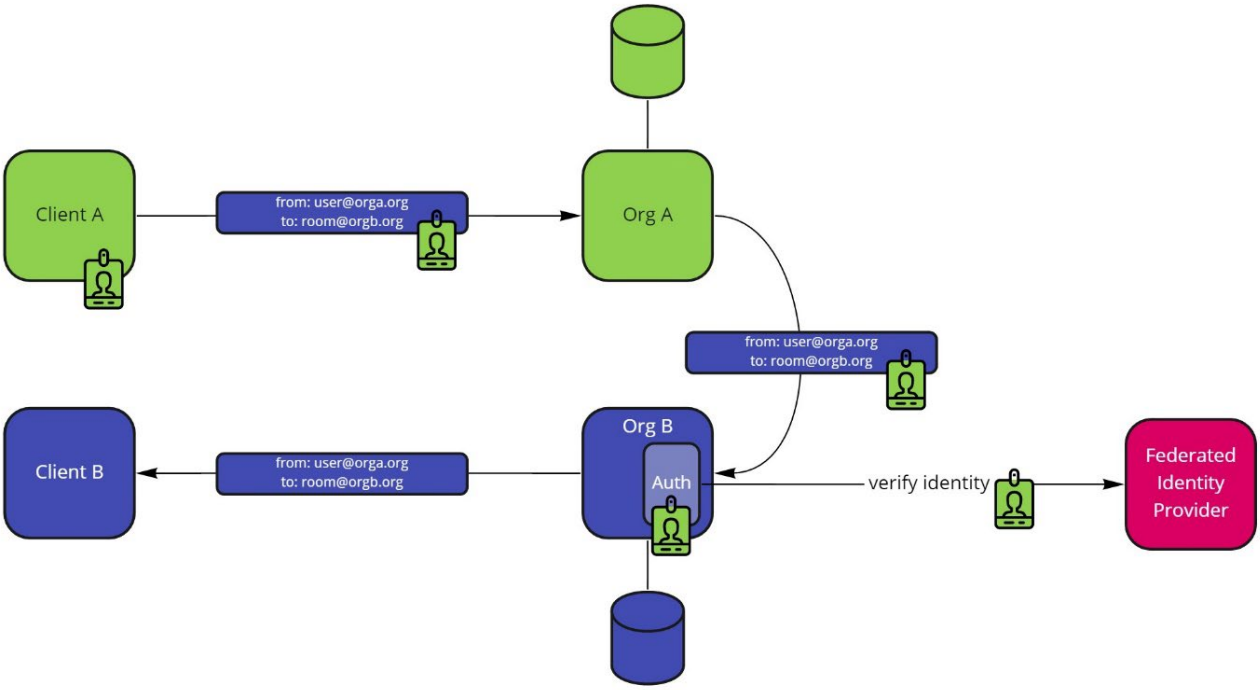
When two organizations have differing representations for classifications with different semantics, the problem of sharing classified information is compounded.

In chat environments manual intervention is not a viable solution, as this prevents real time collaboration. In closely collaborative organizations they may have a common classification scheme, but this is not a universal scenario. An automated system that includes data leakage prevention and classification transformation is required.



Entitlements

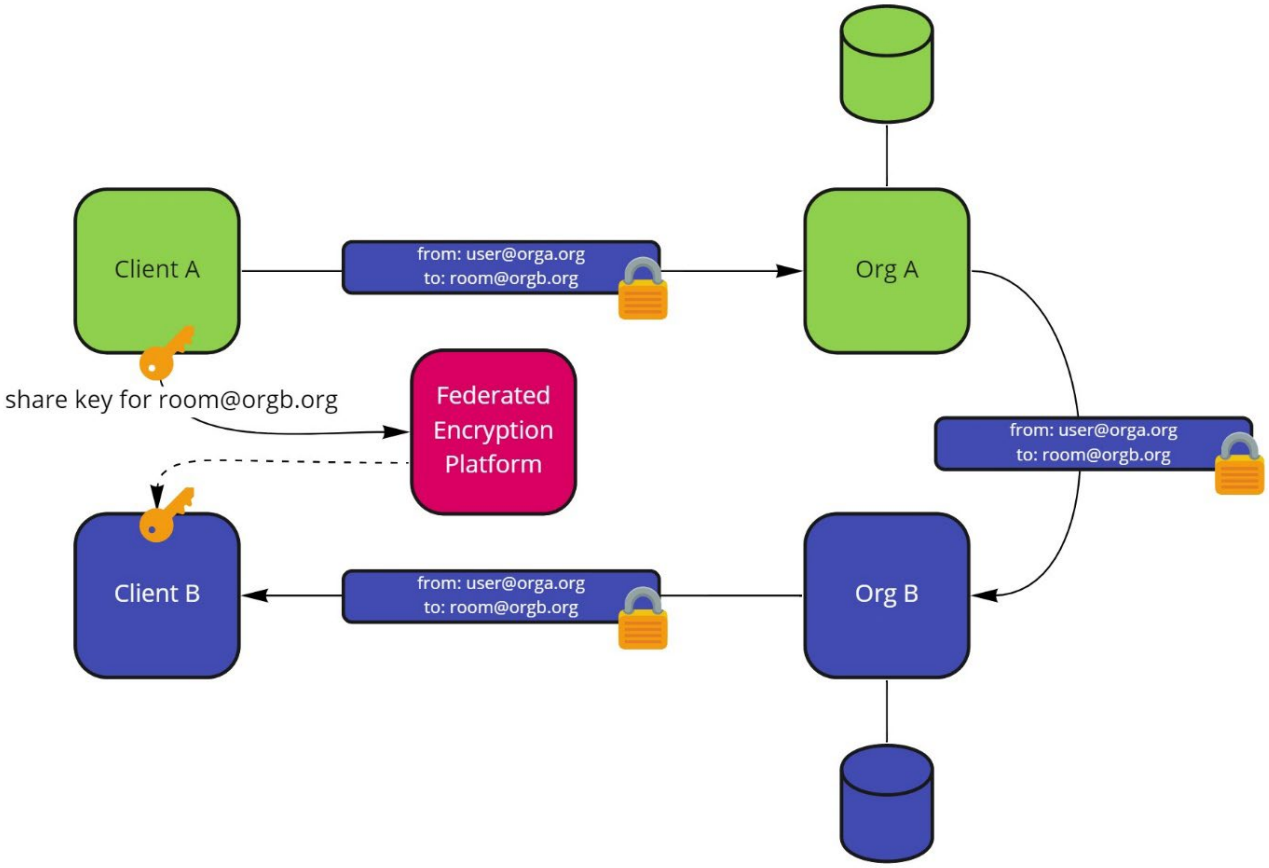
Within an organization, an identity provider (IdP) combined with zero or more entitlement services allow applications to authenticate and authorize users. Across organizations, federated identity providers allow organizations to authenticate individuals from other organizations. The same is not always true when it comes to entitlements, additional controls around sensitivity of entitlements and their semantics are required in scenarios where the *entitlements themselves are protected or classified within an organization*.



In classified environments, the issue of identity is exacerbated, as identities may be pseudonyms and managing permissions using individual identity makes for a difficult-to-manage, constantly moving target. In contrast, leveraging entitlements allows for a more stable mechanism to manage permissions, but requires a solution to federated entitlements.

Encryption

To protect the most sensitive information, end-to-end encryption is necessary. The challenge of encrypting messages end-to-end in a chat room environment has been solved in the consumer space by encrypting room keys for each individual participant in the conversation. This has the effect of requiring a complex system of peer-to-peer trust, a constant online presence of key owners and specialized audit mechanics.

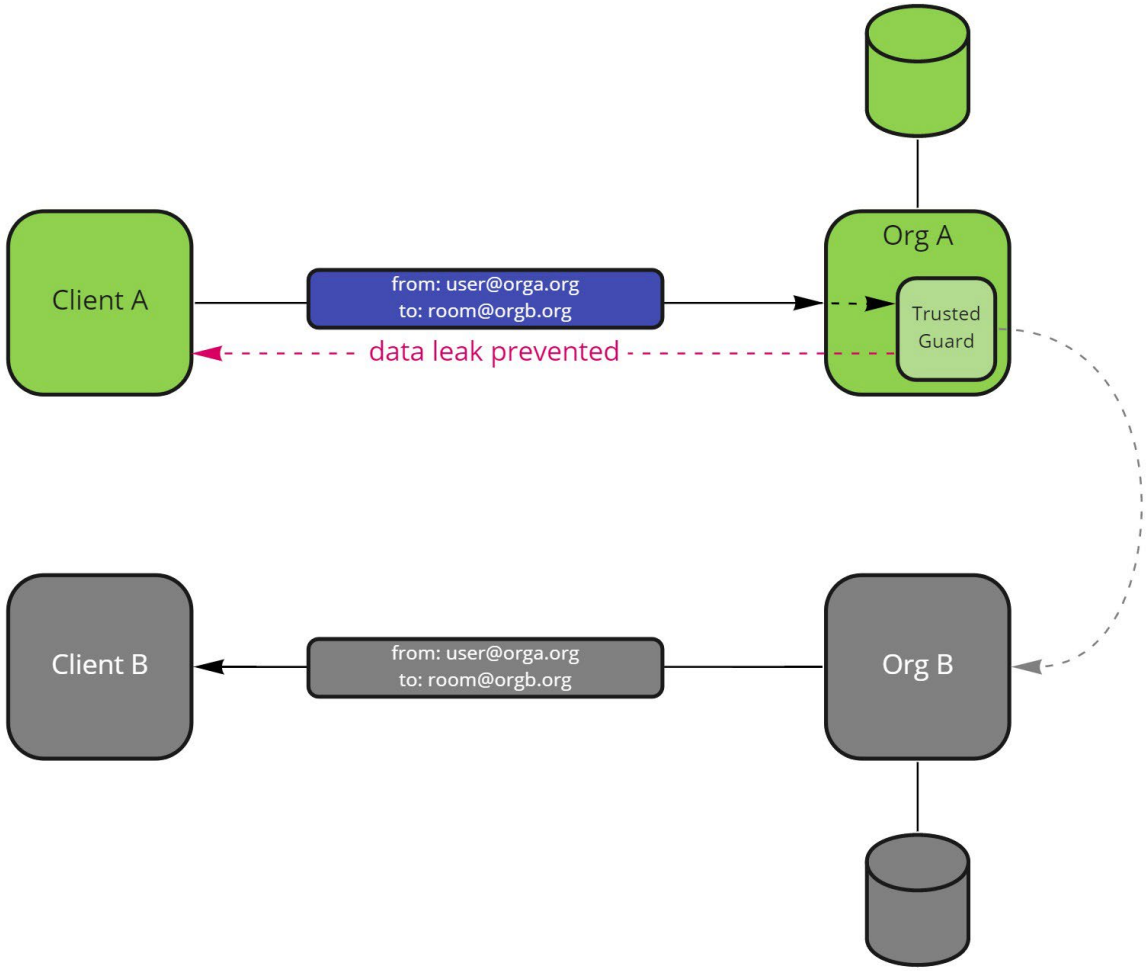


In an organization requiring enterprise governance, an alternative approach is to lean on independent key sharing and key protection systems that enable end-to-end encryption in a room context without the complex requirements of peer-to-peer trust. By leveraging a Communities of Interest (CoI) model, appropriate trust and protection can be established in a scalable way.

Extending end-to-end encryption to a federated environment requires encryption keys to also be shared across organizations. This circles back to the concept of federated identity and entitlements to support key sharing and key protection without introducing account replication. This requires trust at the organization level but is very flexible when it comes to how keys are protected and shared.

Data Leakage Prevention

Any system that allows sensitive information to flow outside of an organizational boundary must address the possibility that attempts are made to leak information out of the organization maliciously or inadvertently. Therefore, any secure, federated solution must employ a **Trusted Guard** that can automatically inspect and intercept information flowing out of the organization to prevent data leakage violations.



The interplay between end-to-end encryption and DLP is a particular challenge that needs to balance a need for true end-to-end encryption and secure, exceptionally classified, federated communication.

Summary

Cross-organization communication, *federation,* is a necessity for the modern workplace. Federated Persistent Chat is a solution that enables *groups of users* in different organizations to seamlessly communicate in a way that respects an organization's governance over its information and the identity of its users.

Extending real-time communication into a secure persistent chat room context that supports federated environments raises a multitude of questions:

- Which organizations host room content and is that content hosted at multiple organizations?
- How do you define members of a room across federated organizations?
- How do you protect sensitivity and control dissemination across federated organizations?
- How do you support end-to-end encryption between federated organizations?
- How do you prevent data leaking or spilling outside of an organization?

MindLink is seeking to extend our core platform with a solution to federation that overcomes the challenges discussed in this whitepaper. By creating a **secure and truly federated persistent chat solution** we believe we can deliver a platform that enables efficient mission-focused collaboration between organizations operating in exceptionally classified scenarios.