

Authorization-Enhanced Email System

Igor Zboran
izboran@gmail.com
August 30, 2020

Abstract

Electronic mail (email) is the most pervasive form of business information exchange. Email is often used not only as an interpersonal communication tool, but also as the default choice to send files. In this paper the User-Managed Access (UMA) authorization framework is proposed to address data storage, access control and data transfer limitations of current email systems. Outgoing mail is typically transferred from the source system to the destination system as a single text-encoded file using Simple Mail Transfer Protocol (SMTP). SMTP is a push protocol only. The UMA framework introduces Resource Server (RS) and Authorization Server (AS) into the email system. The RS is accessed generally by HTTP protocol that was designed as a pull protocol. The two-way push-pull data transfer in combination with a data storage system controlled by the standardized authorization framework significantly leverages email security, enhances email system utilization and elevates the email ecosystem to the ubiquitous Content Services Platform.

Introduction

The main components of the email system have been designed between 1971 and 1992 by many inventors. In the course of time, email has become the most commonly used application of the Internet. Nowadays the email is the only truly decentralized communication system of the Internet and the email infrastructure forms the backbone of the worldwide digital identity.

Problem

Despite the importance of email infrastructure, the whole ecosystem still relies on over 40 year-old architecture and protocol design. There are spam and attachment issues from the very beginning. The email system, while conceptually sound as a communication means, is structurally obsolete and functionally deficient.

Current Situation

With the rising popularity of free email providers, such as Gmail or Outlook.com, web-browsers are increasingly being used to access email server. From a user standpoint, it is easy to read and send email via web-browser on any device, from anywhere in the world. Centralized access to the mailboxes, increases the security of web-based e-mail systems.

Current Flaws

Even though the main email service providers claim email accounts to be safe, the fact remains that major security and functional flaws are not fixed. There is still an attachments delivery dichotomy; the bulky files are not transferred as an attachment but are shared via links. An "attachment sharing" is not natural for postal systems where each message with attachments is expected to be consistent. Shared links pose a consent phishing attack threat where attacker tricks users into granting a malicious application access to sensitive resources. This is known as an OAuth 2.0 authorization exploit. The Authorization-Enhanced Email System (AEES) is resistant to this security exploit as there are no direct user involvement in access granting.

Proposed Solution

Given that email system is lagging behind modern communication and collaboration tools, we propose an OAuth-based access control management and consequently a new data exchange channel for email ecosystem.

Motivation

Email still the most popular communication tool is lacking an important part of today's modern systems – an authorization framework. Understanding this lead us to implement the User-Managed Access authorization framework into email ecosystem.

Main Concept

We propose to incorporate the UMA framework between email system with standardized SMTP/POP3/IMAP interface and proprietary RESTful web-based email application, illustrated in Figure 1.

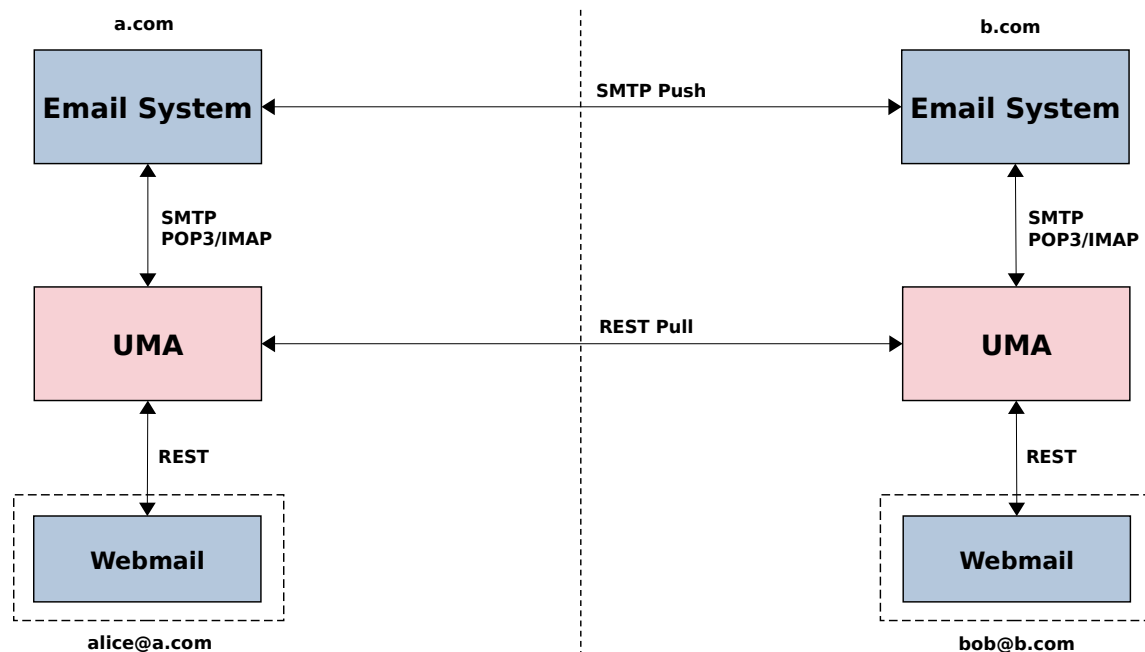


Figure 1. Main concept

Claims:

- On the server side no user content is stored in the messages, only links to the UMA Resource Server (message body link, attachment links).
- The actual content of messages and attachments is stored on UMA Resource Server.
- Webmail application assembles/disassembles email that is stored in Resource Server.
- The user communicates with UMA Resource Server via Webmail application (REST protocol).
- Email is transferred by parts (envelope, body, attachments).
- A user as a sender in a Resource Owner role shares temporary links to the actual message content (disassembled email) with recipients and sends dummy email message with links to Resource Server via email system (SMTP protocol) to recipients. This is done automatically, user always works with assembled email in Webmail application.

- On the recipient side the incoming email with temporary shared links is processed in Mail Fetch Agent (MFA) that acts in Requesting Party role on behalf recipient and actual message content is downloaded from sender's Resource Server and are copied to recipient's Resource Server. Recipient becomes an owner of copied content. The temporary shared links on the sender side are deleted.
- The original email is assembled from recipient's Resource Server data in the recipient's Webmail Application.

Notes:

- This is not a "file sharing by email" system.
- Both senders and recipients have always Resource Owner role. They don't share any data with each other - they hold data copies.
- UMA Requesting Party role belongs recipient's agent – Mail Fetch Agent (MFA) - that acts on behalf recipients and creates data copy using temporary shared links from a dummy email messages.

Trust Model

Figure 2 illustrates the decentralized three-way trust relationship model:

- Mail Trust – SMTP to SMTP trust (the most vulnerable).
- Mail to UMA Trust – a trust delegation from email system to UMA framework.
- UMA Trust – a trust between UMA components.

There is no contract between authorization servers and UMA roles remains co-located.

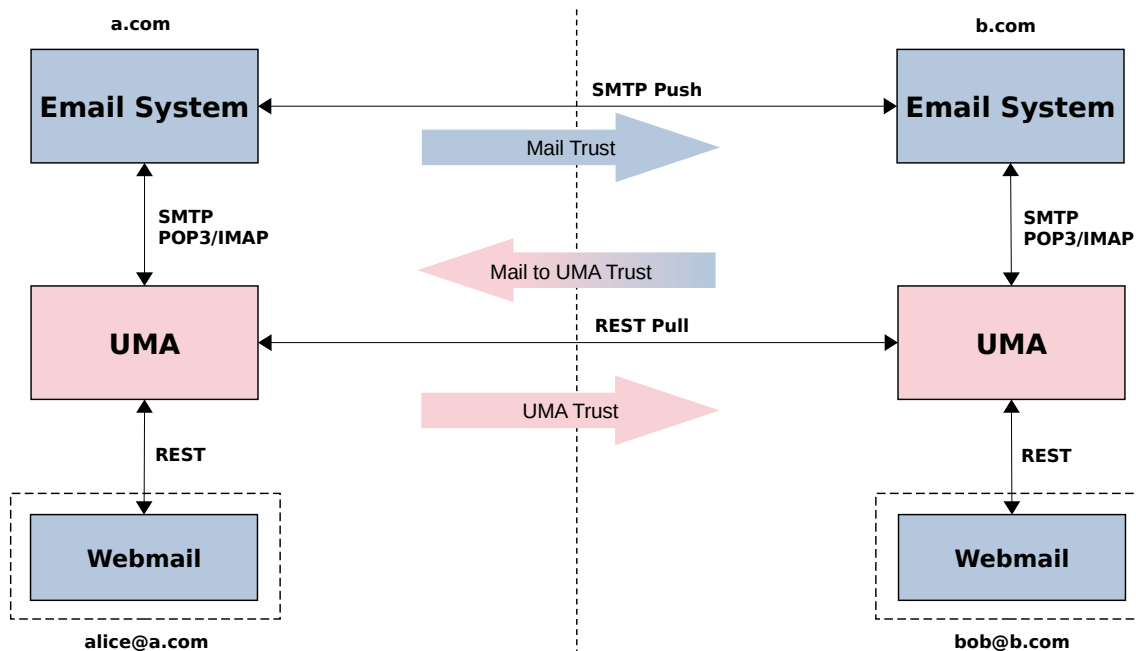


Figure 2. alice@a.com to bob@b.com trust model

Scenarios and Flows

The following scenario represents an email sent from alice.a.com address to bob.b.com address assuming that this is the first ever communication between the a.com and b.com security domains and no trusted relationships is established between them. Trusted communication between users in the two security domains can be divided into seven phases.

Phase I-III.

- get authorization, register, set up a relationship

Before the communication itself, a trusted relationship must be established between b.com MFA in Requesting Party Role and a.com Authorization Server. To set up a relationship a registration email must be sent from a.com domain to the b.com domain. The sending of the registration email must be authorized by a.com Authorization Server. To make this process streamlined OAuth 2.0 Dynamic Client Registration Management Protocol (RFC 7592) is used to avoid manual registration workflow, illustrated in Figure 3. The Initial Access Token and Software Statement are sent in the registration email. This registration email is generated by a.com Resource Server (*who, how, when, ...*).

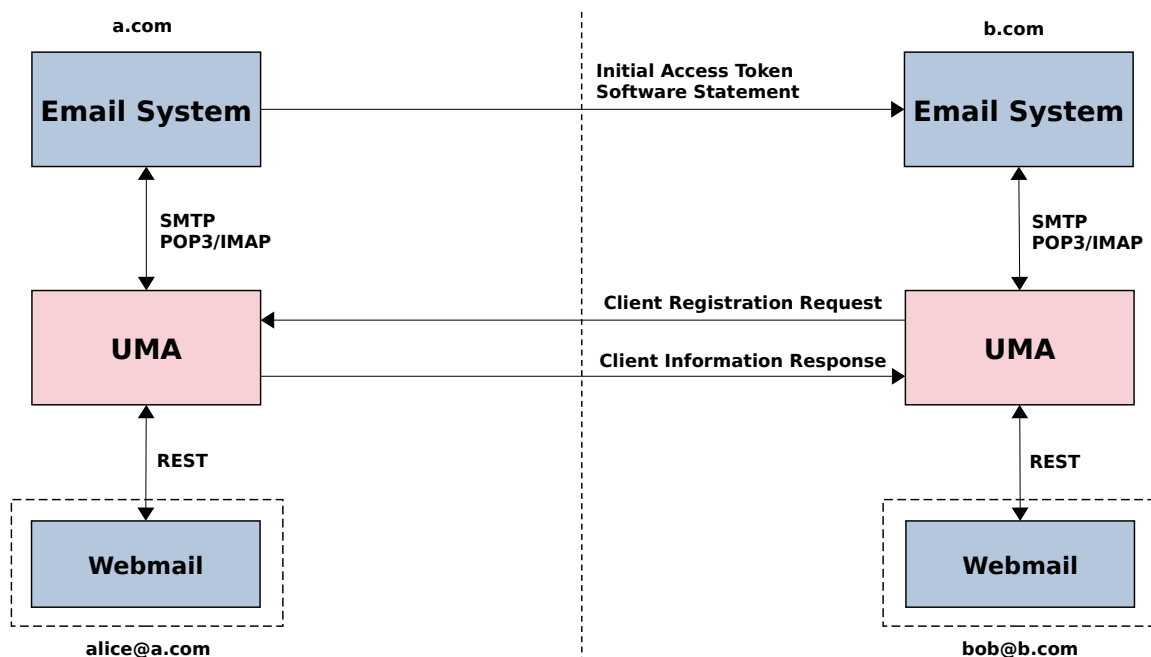


Figure 3. alice@a.com to bob@b.com dynamic client registration

Phase IV-V.

- authenticate, push links

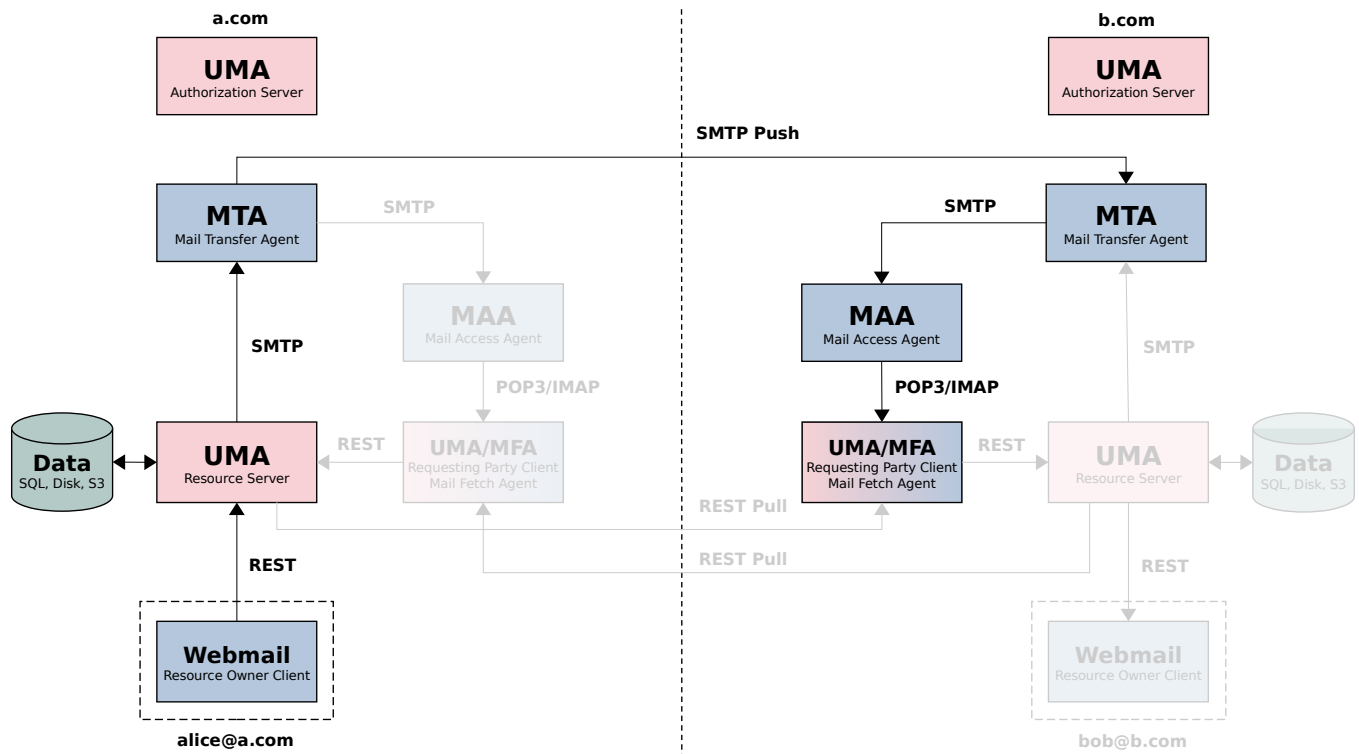


Figure 4. alice@a.com to bob@b.com push links

Phase VI-VII.

- get authorization, pull data

The registration email and user-written email can be merged into one email.

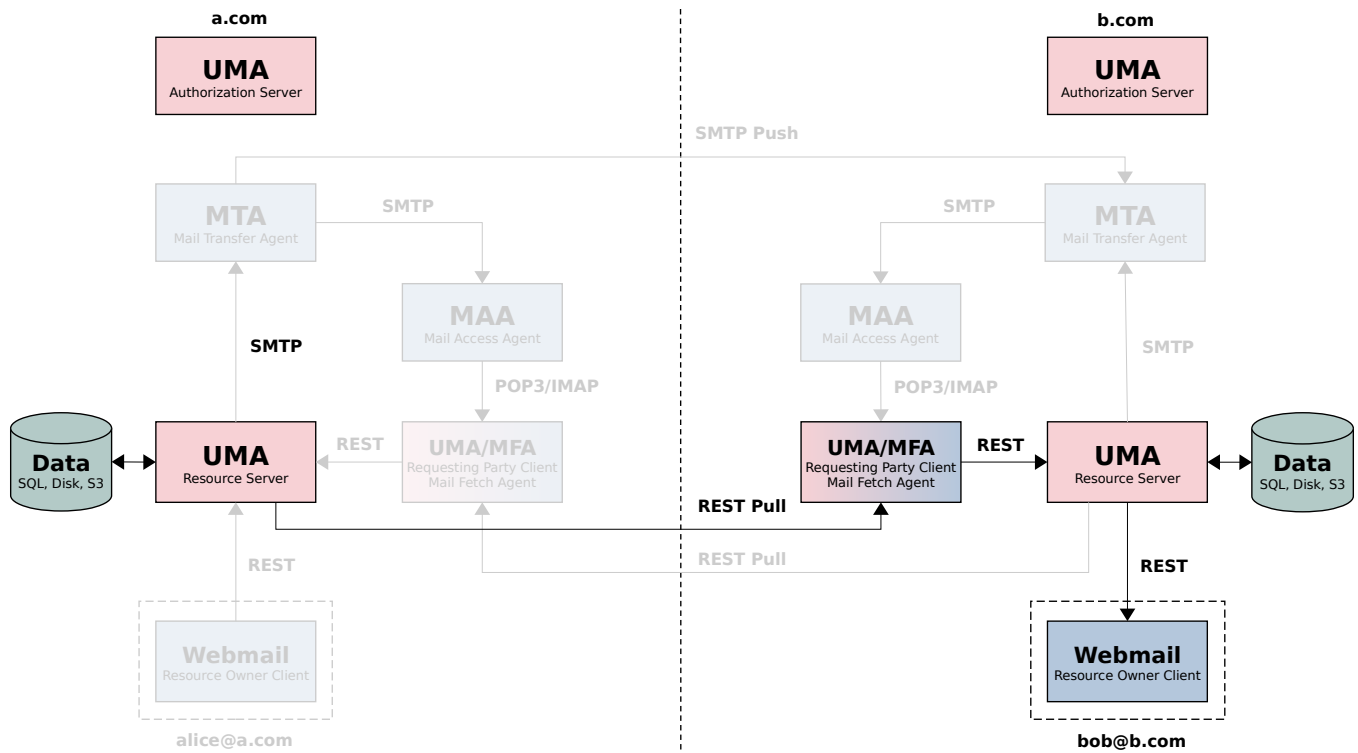


Figure 4. alice@a.com to bob@b.com pull data

Features and Comparison with Current Email System

The novelty of the proposed solution approach can be assessed by comparison with the current email system.

New Features

The proposed AEES solution provides several new features that are lacking in current email systems:

- Intrinsic privacy-preserving properties. Each user can have their own separate email repository (Resource Server). The user can run its own email repository, even its own authorization server.
- Built-in cross-domain autonomic access control via standardized UMA framework.
- No attachments size limit. Attachments are transferred as separate files without size limit.
- Linked content using a clickable hyperlinks.
- Instant messages. Messages and attachments are transferred separately, there is no need to wait for incoming bulky message-with-attachments file. Attachments-stripped bare messages are transferred with a higher priority.

Comparison with Current Email System

From the users point of view, the use of the AEES has many advantages over standard email system. In the following we highlight the advantages of the proposed solution compared to the current email system.

1. Security and Privacy:

The architecture of the AEES guaranties more control over potential security and privacy issues such as leakage of intellectual property or loss of confidential content and makes this system compatible with enterprise security policies.

2. Usability:

At the core of proposed solution is an attempt to improve the usability of email - not only as an interpersonal communication tool, but also as the default choice to send and store files. With the ability to store, locate, send and receive any content including documents, images, audios and videos the proposed solution can be used as a Content Services Platform.

3. Integrations:

The AEES provides a standardized Restful API interface to ease the integrations with external marketing, sales, Enterprise Content Management (ECM) or Customer Relationship Management (CRM) systems.

Conclusion

The AEES has been designed to follow User-Managed Access framework best practices while keeping compatibility with current email systems.

Overall Summary

The Email System technology in combination with User-Managed Access framework creates a composite architecture that meets the needs of the modern communication tool. This architecture increases robustness and performance of existing email ecosystem. The proposed solution can be used as a Content Services Platform to provide the storage repository protected by the standardized authorization framework utilized by users via the Webmail application.

A consolidated access control and a new data exchange mechanism leverages email security and enhances email system utilization. The question arrives whether a standard implementation of UMA can be integrated into the current email ecosystem.

Future Work

The combination of User-Managed Access framework with email system outcomes in a new data exchange technology that predestine email system to become more than a bare messaging tool.

The following are potential future use case areas:

- Consider a Consent mechanism extension design.
- Explore linked content using a clickable hyperlinks – linking content across the business
- Design an extension for exchanging tagged messages and attachments – grouping content across the business
- Design an attachment versioning extension – the attachments with the same content are versioned
- Explore health information exchange between healthcare professionals and inspect use of email communication between patients and healthcare professionals.

A prototype implementation of the AEES could be interesting.

About the Author

Igor Zboran is a mechanical engineer by education with professional experience as a software engineer and solutions architect. He'd like to transform his knowledge into a useful system or service that people would love to use.

Igor received Ing. degree in Mechanical Engineering from the University of Žilina in 1988. After graduating, he worked in several small private companies as a software developer. From 2008 to 2009, he provided expert advice to Prague City Hall IT department as an external consultant. He invented a new decentralized Identity-Based Privacy (IBP) trusted model built around OAuth2 and OpenID Connect standards. Igor is a strong proponent of open source software and open standards.