International Journal of Core Engineering & Management

Volume-7, Issue-11, 2024 ISSN No: 2348-9510

AUTHORIZATION AND AUTHENTICATION PRACTICES IN TELECOM CRM : ENSURING SECURITY AND INTEGRITY IN CUSTOMER RELATIONSHIP MANAGEMENT

Tanmaya Gaur
Bachelor of Engineering (Electronics and Telecommunication),
Birla Institute of Applied Sciences
tanmay.gaur@gmail.com

Abstract

Customer relationship management (CRM) systems help businesses manage interactions with current and potential customers. These systems offer various functions, including customer service, sales automation, and contact management. CRM systems are essential for businesses aiming to improve customer satisfaction, retention, and loyalty, as well as increase sales and revenue. In the telecommunications industry, effective CRM is crucial for maintaining customer satisfaction and loyalty. However, with the growing reliance on digital platforms powered by telecommunication networks and the emergence of various security and fraud threats targeting customers, ensuring the security of customer data is a paramount concern. Legacy organizations often placed inherent trust in their employees when allowing access to customer data, but this is no longer the case. Modern organizations use a hybrid approach that utilizes both customer and employee credentials to determine access. This research paper details the various authorization and authentication concerns when applying such a hybrid approach in a telecom CRM and outlines best practices to safeguard sensitive information and ensure seamless customer interactions.

Keywords— CRM, Telecommunication, Authentication, Authorization, Data security

I. INTRODUCTION

Authentication [1,2] is the process of verifying the identities of people, apps, and services before giving them access to digital systems and resources. It is an essential part of cybersecurity, helping organizations protect their systems, data, networks, websites, and applications from attacks. Common authentication methods include passwords, biometrics, and multifactor authentication.

Authorization [1,2] is a critical aspect of cybersecurity, ensuring that only the right people, services, and apps with the right permissions can access organizational resources. It typically involves three primary steps: identification, authentication, and authorization. Various methods such as passwords, biometrics, certificates, and multifactor authentication are used to protect identities and prevent unauthorized access

All traditional applications use session management techniques to securely store and utilize the user's authentication and authorization profile, which drives their application session and level of access. Figure 1 below represents user authentication and authorization for a traditional web application.

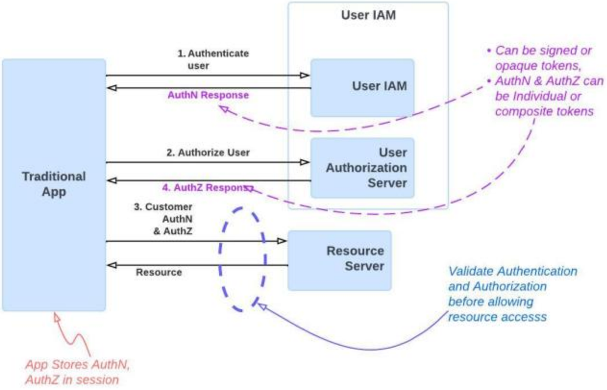
User IAM
1. Authenticate user
AuthN Response
User IAM
• Can be signed or opaque tokens,
• AuthN & AuthZ can be Individual or composite tokens
Traditional App
2. Authorize User
User Authorization Server
4. AuthZ Response
3. Customer AuthN & AuthZ
Resource Server
Resource
Validate Authentication and Authorization before allowing resource accesss
App Stores AuthN, AuthZ in session

Fig 1 Traditional Application Authentication and Authorization

However, in a CRM, there are additional complications due to the involvement of multiple actors. Typically, a CRM transaction involves both an end customer and a company employee. The end user must authenticate and may have specific authorization levels based on their user profile or regulatory compliance laws to be able to request employee to perform transactions. Similarly, the company employee must authenticate to access the CRM and generally has a specific set of authorizations that dictate their actions. These authorizations may be driven by the employee's profile, line of business, role, and regulatory concerns.

This paper will take some of these additional CRM considerations and highlight how these nuances impact CRM designs to get to a possible strategy. Before we dive into considerations with Customer Identity management (CIAM) and Employee Identity management (EIAM), lets first discuss general session management practices and how session information like authentication and authorization is stored.

II. CRM SESSION MANAGEMENT CONSIDERATIONS

Session management involves maintaining a consistent session between the client and server by storing a secure token on the client application, which is then included with all HTTP trafficand is well understood by the server. As an example, for an amazon.com commerce flow, the session management token encapsulates the trusted user identity based on authentication credentials.Where necessary, it is common practice to tokenize and hold the authentication and authorization credentials of the user in the session. Let's go over some considerations in storing this information.

A. JWT v/s Opaque Tokens

With the understanding that the session tokens are representative of secure session information between client and server and play a role in the authentication and authorization of the user. Let's discuss the two popular types of session tokens

- Opaque tokens have a longer history with web development and is usually an alphanumeric string that identifies some information in the database of the issuer.
- JWT Tokens on the other hand is a JSON string that contains all the claims and information it represents and is certified by a signature from the issuer. By default, it's unencrypted, but it can be encrypted via the JSON Web Encryption (JWE) standard.

Given the different nature of these tokens, there are nuances which developers must consider. Opaque tokens are essentially unique random strings and hence useful for transmitting sensitive information which should not be available to the client. They also have significant advantages when it comes to revoking the tokens as well as payload size since the data is all stored server side.

JWT Tokens on the other hand have advantages for highly distributed systems. An application does not have to repeatedly query the authorization server to retrieve token details as JWT token are signed and can be validated locally. This could be a crucial when you are building applications for performance and scale. This makes JWT a shiny alternative in case the session data does not contain sensitive information, and tokens don't need to be revoked.

B. Encryption and Data Protection

- Data Encryption: To protect sensitive customer data, telecom CRM systems employ robust encryption techniques for data at rest and in transit. Encryption ensures that even if data is intercepted or accessed by unauthorized parties, it remains unreadable without the appropriate decryption keys. Advanced encryption standards (AES) and Transport Layer Security (TLS) are commonly used protocols in telecom CRM systems.
- Tokenization is a process that substitutes sensitive data with unique identifiers or tokens. These tokens can be utilized within the CRM system without revealing the actual data, thereby reducing the risk of data breaches. Tokenization is especially beneficial for managing payment information and personally identifiable information (PII) within telecom CRM systems.

C. Types of Tokens

Now that the paper has discussed the intent of the session tokens, let's talk about the various types of tokens needed in enterprise applications.

- Access tokens are the most common and are generally issued by an authorization server. These can be opaque of JWT even though there is widespread misconception assuming Access tokens are always Opaque. These are traditionally issued for small durations to prevent against hijacking, a topic that will come up later in this paper. Access tokens are often used as bearer tokens where the bearer of the token is granted access to specific API(s) and data.
- ID Tokens are part of the OIDC spec and represent the user identity and authentication metadata. These are always JWT and may contain multiple properties and claims standardized for the enterprise like the issuer (who issued the tokens) , actor (who is using the tokens) , subject (identity of the user token is being used for. Often the same but in certain case like a CRM, subject and actor may be different. Actor could be a customer service agent, and the subject is the subscriber account the agent is working on) and expiry associated with the token.
- Refresh Tokens are tokens that allow a client to invoke a refresh flow for the access tokens. The access token is purposefully given short lifetimes. The refresh tokens allow for ways to obtain a new Access token securely without having the user re-authenticate.
- Access tokens and bearer tokens can be vulnerable to be stolen and are often bound to the client/device/machine to which it was issued. This kind of tokens binding the Access token or requests to the client/device/machine is often known as the Proof-of-Possession tokens. MTLS is another strategy used to create sender constrained tokens.

In case of a CRM, the need to hold both the agent and customer in the session, as well as supply them in the request when invoking API(s) ends up with two options

- Overload the Access and ID Token to hold both sets of information. While ideal, this often runs into complications if there are two different IAM solutions for agent and customer.
- Let the Access token and ID Token represent the employee and introduce additional custom token to handle customer data.

D. Authentication Practices

A CRM often handles two sets of authentications[3,4]. First, the employee authenticates by providing some Authentication Methods References (AMRs) and possibly a second factor. Then, when the employee looks up a customer, they may need to provide some customer AMR, which is often supplied by the customer.

- The AMR (Authentication Methods References) are the identifiers for authentication methods used during the authentication event. As an example, if a customer verifies by providing a Govt issued ID, the ID is the AMR.
- Password Management and Policies : Effective password management is a cornerstone

of authentication practices in telecom CRM systems. Organizations enforce stringent password policies, such as requiring complex passwords, periodic changes, and prohibiting the reuse of old passwords. Additionally, telecom companies often implement password management tools that help users generate and store strong passwords securely.

- Multi-Factor Authorization (MFA) adds an additional layer of security by requiring users to provide multiple credentials before accessing sensitive CRM data. Typically, this involves something the user knows (password), something the user has (security token), and something the user is (biometric verification). Multi-Factor Authentication (MFA) greatly diminishes the risk of unauthorized access, even if one authentication factor is compromised.
- Single Sign-On (SSO) streamlines the authentication process by enabling users to access multiple CRM applications with a single set of credentials. This approach not only improves user convenience but also mitigates the risk of password fatigue, where users might choose weak passwords due to the challenge of remembering multiple credentials. SSO integrates seamlessly with existing security infrastructure, ensuring that authentication processes remain robust and secure.
- Biometric Authentication is increasingly being adopted in telecom CRM systems as a means of verifying user identities based on unique biological characteristics. Common biometric methods include fingerprint scanning, facial recognition, and voice authentication. Biometric authentication offers a high level of security and convenience, making it difficult for unauthorized users to gain access.
- Behavioral Biometrics : In addition to traditional biometrics, behavioral biometrics analyze patterns in user behavior, such as typing rhythm, mouse movements, and even navigation habits within the CRM [6] system. This continuous authentication method ensures that the user remains authenticated throughout the session, providing an added layer of security against session hijacking and unauthorized access.

E. Authorization Practices

User authorizations refer to the process of granting or denying specific permissions to users for accessing resources or functionalities based on their identity and role within a system. This concept is crucial in ensuring the security and integrity of an application.Listed below are some key authorization considerations for building out an application. As mentioned, CRM(s) often must apply authorizations from perspective of both the employee as well the customer, specificities we will break down in subsequent sections.

- User authorizations are often discussed in the context of projects and security configurations. This is a fundamental concept in information security and access management and involves determining who can access specific resources and what actions they can perform. This process typically follows authentication, where a user's identity is verified. Once authenticated, the system evaluates the user's roles, permissions, and any specific conditions to decide whether to grant or deny access.

- Most applications that need to scale tokenize the user's authorizations, which is then supplied in subsequent resource requests. This allows downstream resource servers to then apply the authorization rules before responding.
- Role-Based Access Control (RBAC) is a commonly used authorization mechanism in telecom CRM systems. It grants permissions to users based on their roles within the organization. For example, customer service representatives might have access to customer interaction logs, while managers could have broader access to analytics and reporting tools. RBAC ensures that users can only access the information necessary for their specific job functions, thereby minimizing the risk of unauthorized data access. This approach is effective when considering only the employee's authorizations.
- Attribute-Based Access Control (ABAC) provides a more granular approach to authorization by considering various attributes, such as user roles, time of access, and the sensitivity of the data. This dynamic method allows telecom companies to implement more sophisticated access control policies. For example, an employee may have access to certain customer records only during business hours or from specific IP addresses, enhancing security measures. This approach is necessary to be able to apply controls based on both employee and customer authorizations.

F. Compliance and Regulatory Considerations

Aside from authorization and authentication practices, Regulatory guidance guidesthe application implementations. A good example of a data privacy guideline would beGeneral Data Protection Regulation (GDPR) which imposes strict requirements on the handling and protection of personal data for organizations operating within the European Union. Telecom companies operating in European Unionalso need toensure that their CRM and other systems comply with GDPR provisions like obtaining explicit consent from customers, implementing data protection measures, and providing mechanisms for data access and deletion upon request.

Another type of regulations are the ones issues by the country's telecom authority. Different countries have their own regulatory bodies that oversee telecommunications practices. For instance, the Federal Communications Commission (FCC) in the USA regulates communications by radio, television, wire, satellite, and cable across the United States. The FCC also provides guidelines on data protection, customer privacy, and cybersecurity.

In addition to federal entities, there are often state level guidelines and protection rules issues by states which may apply to telecom companies. A example (USA) would be California Consumer Privacy Act (CCPA) applied by state of California which is very similar to GDPR and targets to provide end consumers control over the personal information that businesses collect about them , CCPA regulations provide guidance on how to implement the law.

There are at times more targeted laws like the Cybersecurity Maturity Model Certification

(CMMC) model, which is designed to protect Federal Contract Information (FCI) and Controlled Unclassified Information (CUI) that is shared with contractors and subcontractors of the Department through acquisition programs.

Telecom companies must understand and adhere to all such guidelines to maintain their operating licenses and ensure customer trust. The CRM Tools often need to have specific additional authorizations and implementations to handle these regulations on top of the authentication / authorizations

III. EMPLOYEE AUTHENTICATION AND AUTHORIZATION CONSIDERATIONS

For most enterprise employees, authentication and authorization strategies [5] are designed to ensure secure access to the enterprise systems and data while providing a seamless user experience.

- Most organizations in this digital age employ multi-factor authentication (MFA) approaches, which may include biometric authentication, such as facial recognition and fingerprint scanning, as well as traditional methods like passwords and security tokens. This multi-layered security approach helps protect against unauthorized access and data breaches. This shift aims to enhance security and reduce the risk of password-related vulnerabilities.
- It is recommended for identity management solutions to follow least privilege principles and practicing separation of duties, ensuring that employees have access only to the resources they need for their roles. This is especially important for CRM solutions.
- Active Directory security groups are commonly used to grant users permissions to IT resources and can also be utilized in CRM systems. Each security group is assigned a specific set of access rights, and users are added to the appropriate groups. When implemented correctly, this approach can facilitate an accurate, role-based method for managing CRM users.
- It is recommended to conduct regular security risk audits and assessments to validate the access controls.
- Authorizations are another critical component of the company's security infrastructure, ensuring that access to sensitive information and systems is tightly controlled. Role and Entitlement based authorization servers are often used to provide centralized, fine-grained authorization through policy-based access control (PBAC), allowing administrators to create detailed policy objects that define who can access what resources, under what conditions, and when.
- CRM systemsfirst authenticate users and then enforce authorization policies. This integration ensures that only authorized personnel can access specific applications and data, enhancing security across the organization.
- There are always employees with elevated access controlled by authorization entitlements, which allows them to overrise and bypass certain controls. As an example,

back-office admin users may be allowed to pull up a customer account without verification.

IV. CUSTOMER AUTHENTICATION AND AUTHORIZATION CONSIDERATIONS

Once an employee looks up a customer account, customer lookup and verification strategies ensure secure access to the customer data. This process verifies that the agent is authorized to access the customer account and confirms that the person requesting access is indeed the customer and not a fraudulent actor. Overall, these controls are part of a comprehensive security strategy to safeguard customer data and ensure that only verified and authorized interactions occur in the CRM environment. Some CRM nuances are listed below

- Customer lookup and verification controls in CRM are designed to ensure secure and efficient handling of customer information. These controls involve multiple layers of authentication and verification to protect against fraud and unauthorized access.
- One key aspect is the use of tokens to encapsulate the customer verification status. These tokens are sent with API requests to retrieve data. Depending on the company's support setup, these tokens may also be passed between agents to handle scenarios like call transfers.
- Additionally, when the CRM system integrates with various backend databases and APIs to retrieve and validate customer information, these tokens are recommended to be validated by these backend APIs to confirm verification status before returning requested information.
- Moreover, the CRM and backend systems can employ role-based and attribute-basedaccess controls to ensure that only authorized customers can request certain actions. This includes blocking high-risk transactions, such as SIM changes, for users who do not have the necessary permissions

V. RECOMMENDED CRM APPROACH

So, what should a CRM approach look like. Figure 2 below represents one implementation strategy. As we discussed in going over the various considerations, the enterprise needs and requirements should drive the solution. As an example, should you use one composite token or multiple tokens? Most of the answers lie in your CRM specificities.

In the below example, the CRM first interacts with the employeeIAMto generate an employee token, and then with the customer IAM to generate a customer token. Both these tokens are supplied in subsequent requests where they are validated before allowing resource access.

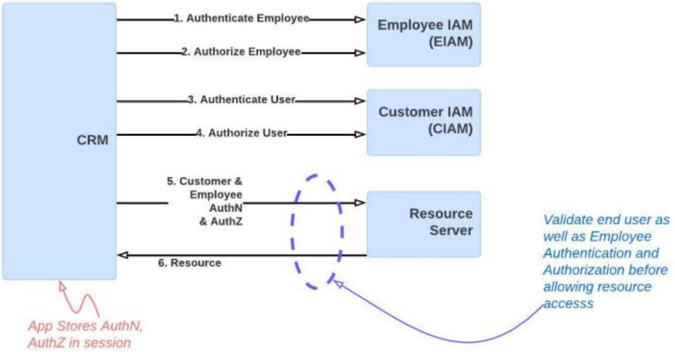
1. Authenticate Employee
2. Authorize Employee
Employee IAM (EIAM)
3. Authenticate User
4. Authorize User
Customer IAM (CIAM)
CRM
5. Customer & Employee AuthN & AuthZ
Resource Server
6. Resource
Validate end user as well as Employee Authentication and Authorization before allowing resource accesss
App Stores AuthN, AuthZ in session

Fig 2 CRM Authentication and Authorization

VI. LIMITATIONS/CHALLENGES AND FUTURE SCOPES

Unlike standard IAM practices, CRM authentication and authorization processes are not uniform. This is due to the various technical, functional, compliance, and behavioral differences and limitations across different CRM scenarios. With the introduction of increasingly complex products and services, this space is becoming even more complicated. It is prudent for companies to thoroughly understand their scope and needs, stay updated on the latest developments in fraud, security, and compliance, and ensure their strategies are appropriate and continuously evolving to meet these needs.

Advancements in AI/ML, including technologies like AI Bots, add another layer of complexity to this already challenging topic. Determining the appropriate level of access, how these new experiences should be authenticated and authorized, and how this evolves with the move to automation are all critical considerations. This is an evolving area that organizations need to be particularly mindful of.

VII. CONCLUSION

This document coveredconsiderations for authentication and authorization strategy of a modern customer relationship management (CRM) systems in the telecommunications industry. As discussed in the manuscript

- It is important to setup robust and hybrid authentication and authorization mechanisms across employee and customer profiles to adequately protect sensitive customer data and ensure seamless interactions.
- It is important to considerhow common authentication methods such as passwords are now inadequate on their own and need to apply alongside other multi-factor

authenticators like biometrics. This is true both for the agent authentication as well as the customer verification.

- It is recommended to employ the hybrid authorization approach integrating both employee and customer profiles to generate and validate tokens at not just the CRM UI but across backend API(s) and databases, ensuring secure and efficient enterprise operations.

REFERENCES

1. Authentication and Authorization Explained https://auth0.com/docs/get-started/identity-fundamentals/authentication-and-authorization
2. Differences between Authentication and Authorization https://www.sailpoint.com/identity-library/difference-between-authentication-and-authorization
3. CRM Core Roles with Authentication and Authorization https://community.auth0.com/t/crm-with-auth0-authorization-core-roles/61985
4. Identity and Access Management https://www.cdw.com/content/cdw/en/resources/identity-access-management-mkt10806.html
5. Authentication strategy for modern web applications https://www.sciencedirect.com/science/article/pii/S1877050922021512
6. Synergy of CRM with business strategy and architecture https://www.linkedin.com/pulse/whitepaper-synergy-crm-customer-relationship-management-sg-/
7. Jacobs, S., 2013. Security management of next generation telecommunications networks and services (Vol. 14). John Wiley & Sons.
8. Chan, S.S. and Lam, J., 2005. Customer relationship management on internet and mobile channels: an analytical framework and research directions. E-commerce and M-commerce technologies, pp.1-31.
9. Al-Weshah, G.A., Al-Manasrah, E. and Al-Qatawneh, M., 2019. Customer relationship management systems and organizational performance: Quantitative evidence from the Jordanian telecommunication industry. Journal of Marketing Communications, 25(8), pp.799-819.
10. Varone, N. and Albayrak, S., Towards Customer Relationship Management Systems for Financial Services based on Agent Technology.
11. Ghaleb, a., 2018. Customer relationship management and customer retention in y-telecoms (doctoral dissertation, lebanese international university).