# How to secure data with the Asset Administration Shell

**Juilee Tikekar**

*The phrase "Data is the new oil" was coined by British Mathematician Clive Humby in 2006. This phrase makes clear that, just like oil, the data cannot be used in its raw state, it needs to be collected, standardized, and turned into meaningful information.*

*For asset-oriented industries, the ability to access and share information, e.g., process information (IT), asset monitoring information, etc., throughout the lifecycle in an interoperable manner is essential. One way to achieve this goal is with the help of digital twins.*


Figure 1: XML-Signature in AAS Structure [8].

A digital twin is a digital representation of an asset, whereas Asset Administration Shell (AAS) is a specific such representation standardized as IEC 63278 [1]. Thus, IT/OT convergence through digital twins with the help of AAS offers benefits including increased transparency and interoperability. However, in addition to these benefits, security is considered as a significant factor.

## Defining the security oft the AAS

Therefore, the Task Force "Security" of the working group "Open Technology" in the Industrial Digital Twin Association (IDTA) is working on defining the security of the Asset Administration Shell (AAS). The results of this Task Force will be published as Part 4: Security of the "Specification of Asset Administration Shell" series [2]. This security-related specification targets data leakage protection, consistent data exposure, protection against modification of the data by unauthorized parties, thereby supporting the integrity and accountability of the data and protection against malicious hiding of the data.

The security of AAS considers two main use cases of exchanging the information via AAS i.e., Type 1 (exchange as an AASX File [3]) and Type 2 (access to AAS by API [4]). The security in both cases can be handled by a Security Model. Additionally, in the case of AASX File exchange, an AASX can be digitally signed (XML Signature) for authenticity protection. By this an application can prove the authenticity while reading the AASX. An example of the AAS structure can be seen in Figure 1. While handling AASX files with signatures, AASX encryption is currently not considered under the scope of standardization.

In the case of access to AAS by APIs, the provider of an AAS or Submodel needs to define access control for multiple roles and individual resources. Therefore, authentication and authorization are important in AAS Servers. The AAS Servers may provide data available to anonymous users or restrict certain data to some users. In such a case, first, the user application/client needs to authenticate itself to an Identity Provider (IP) and receive an access token. This access token is a JSON Web

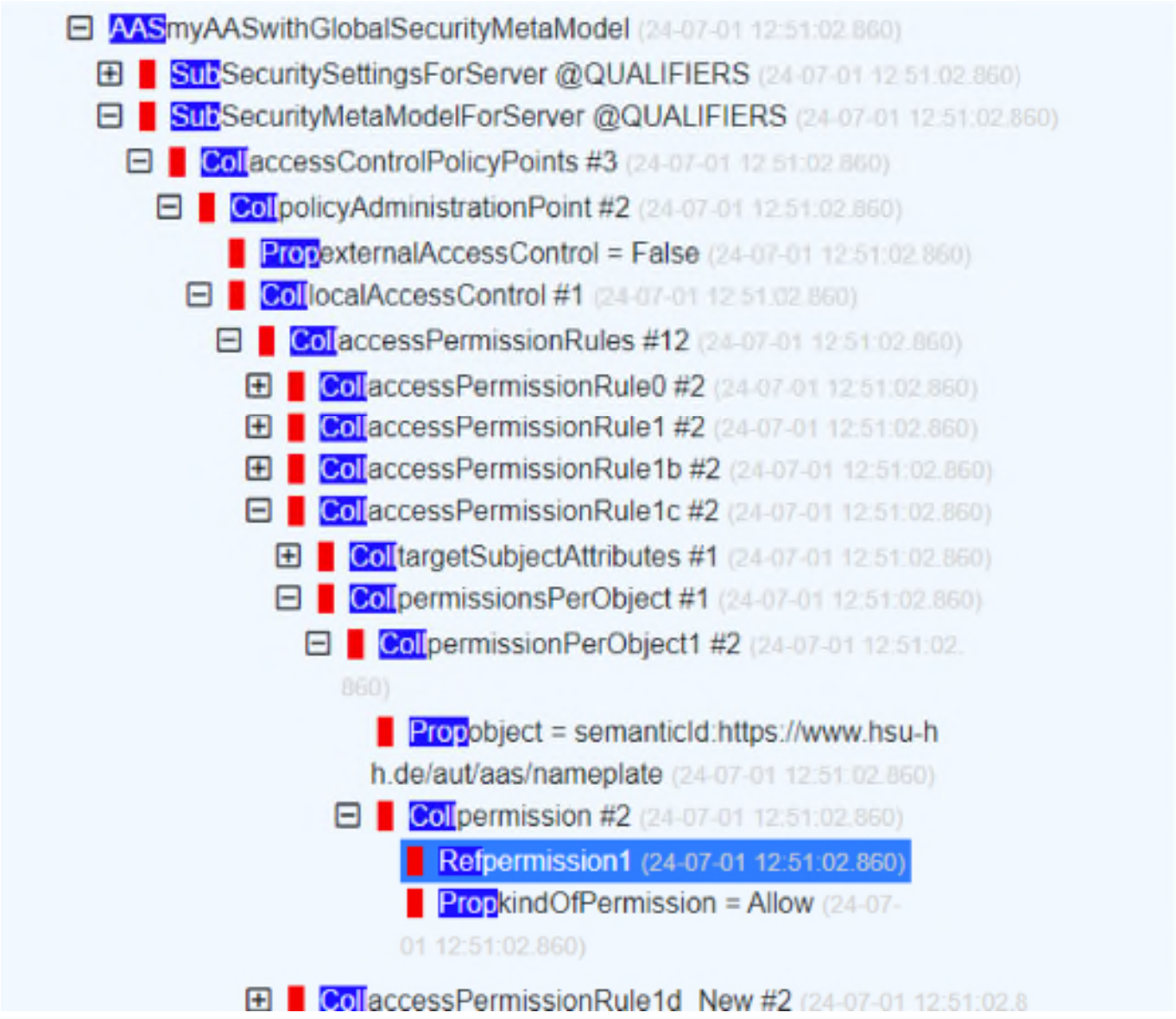


Figure 2: Access Rules in AAS Format [9].

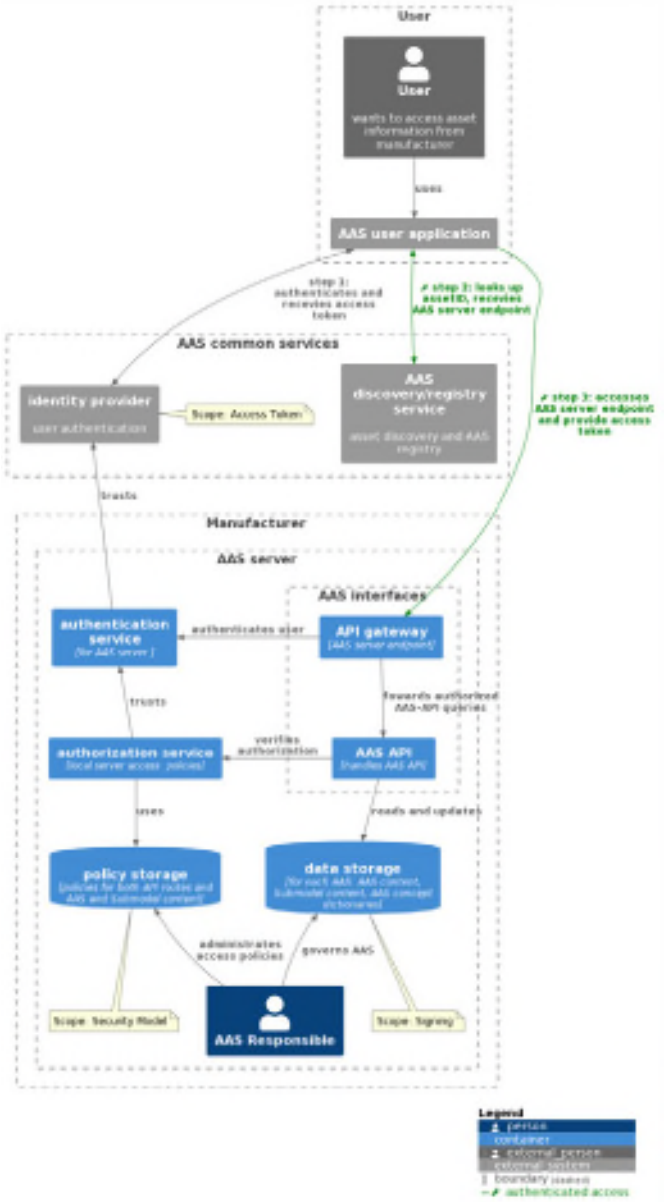


Figure 3: Example of server implementation [8].

Token (JWT) according to RFC 7519 [5]. This access token will then be used by the AAS Server or API Gateway to verify the signature of the access token. Once the authentication is successful, the AAS Server will perform the authorization.

This authorization can be based on Attribute Based Access Control (ABAC) [6] and will be carried out in two stages. In the first stage, the authorization against the API route will be executed, whereas in the second stage, the authorization against the request AAS element will be executed. The access rules for authorization can be defined for API Routes, and AAS elements such as Identifiables, Referables, and SemanticIds. Additionally, it is possible to store these access rules in AAS Format (see Figure 2) as well as in a proprietary way by AAS Server. Figure 3 demonstrates a possible server implementation with this approach.

## Example implementation ZVEI Showcase DPP4.0

An example implementation of these concepts has been included as part of a several demonstrations such as ZVEI Showcase DPP4.0 [7]. The current focus of the Task Force is the interaction between external and internal Identity Providers. The results of the Task Force will also brief us about the role of AAS security in dataspaces, which will ensure the exchange of data securely and in an interoperable manner.

## References

[1] Industrial Digital Twin Association. (2024). Specification of the Asset Administration Shell – Part 1: Metamodel. Retrieved from: https://industrialdigitaltwin.org/wp-content/uploads/2024/06/IDTA-01001-3-0-1_SpecificationAssetAdministrationShell_Part1_Metamodel.pdf

[2] Industrial Digital Twin Association. (2024). AAS specifications. Retrieved from: https://industrialdigitaltwin.org/content-hub/aasspecifications

[3] Industrial Digital Twin Association. (2024). Specification of the Asset Administration Shell – Part 5: AASX Package File Format. Retrieved from: https://industrialdigitaltwin.org/wp-content/uploads/2024/06/IDTA-01005-3-0-1_SpecificationAssetAdministrationShell_Part5_AASXPackageFileFormat.pdf

[4] Industrial Digital Twin Association. (2024). Specification of the Asset Administration Shell – Part 2: API. Retrieved from: https://industrialdigitaltwin.org/wp-content/uploads/2024/06/IDTA-01002-3-0-2_SpecificationAssetAdministrationShell_Part2_API.pdf

[5] Internet Engineering Task Force (IETF). (2015). JSON Web Token (JWT). Retrieved from: https://datatracker.ietf.org/doc/html/rfc7519

[6] Hu, V. C., Ferraiolo, D., Kuhn, R., Friedman, A. R., Lang, A. J., Cogdell, M. M., ... & Scarfone, K. (2013). Guide to attribute based access control (abac) definition and considerations (draft). NIST special publication, 800(162), 1-54. https://doi.org/10.6028/NIST.SP.800-162

[7] Industrial Digital Twin Association (IDTA), ZVEI. (2024). DPP4.0 – The Digital Product Passport for Industry 4.0. Retrieved from: https://dpp40.eu/

[8] Phoenix Contact. (2024). Security of the Asset Administration Shell. Retrieved from: https://h2894164.stratoserver.net/aas-und-security/240422_1505_Orzelski_Andreas_PhoenixContact_Security_of_the_AAS.pdf

[9] Industrial Digital Twin Association (IDTA). AASX Browser. Retrieved from: https://v3security.admin-shell-io.com/

**Juilee Tikekar**
Digital Twin Expert
Industrial Digital Twin Association (IDTA)
60258 Frankfurt am Main

**Alexander Orzelski**
Master Specialist Standardization
Phoenix Contact
32825 Blomberg