User-Managed Access (UMA)

Degree programme: BSc in Computer Science | Specialisation: IT-Security
Thesis advisor: Prof. Dr. Reto Koenig
Expert: Prof. Dr. Andreas Spichiger

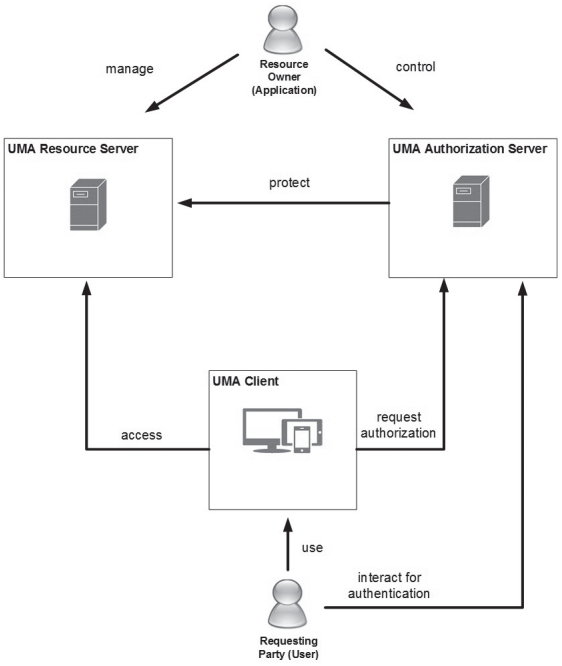
In the future more and more user data will be moved from private storage to the cloud. To share and protect this data in a secure manner new protocols and standards are needed. Existing models such as OAuth 2.0 already enable lots of opportunities but have their limitations. User-Managed Access (UMA) takes access control to the next level and provides an adaptive solution to maintain control over your data.

Initial Situation

Based on our previous work we evaluated an OAuth 2.0 profile called «User-Managed Access (UMA)» for Velospot Biel to control IoT-data of bicycles. In our thesis we continue to explain and understand the functionalities and peculiarities of UMA. In the beginning, we had planned to develop a full implementation of UMA and its components. But as the specification is in an ongoing process of rewriting and restructuring we proceeded by analyzing the protocol and tried to support the continuous progress of becoming a web standard.

What UMA does

With UMA a Resource Owner is able to manage protected resource access by a Requesting Party and their UMA-Client in an asynchronous fashion. The resources which the Resource Owner wants to protect can be hosted on several Resource Servers. The access management is done by a central Authorization Server which is controlled by the Resource Owner. This introduces the possibility to keep policies for various unrelated Resource Servers in one location.



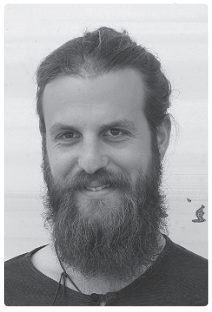
UMA components and their actions

Our Work

Approaching UMA from both a theoretical and a practical point of view we strove for a better understanding of the security mechanisms and their potential impact. On the theoretical level we looked into the specified features by introducing a genuine story to perceive how UMA is built. In a further step we implemented parts of the protocol to get more insights into the decisions the architects made.

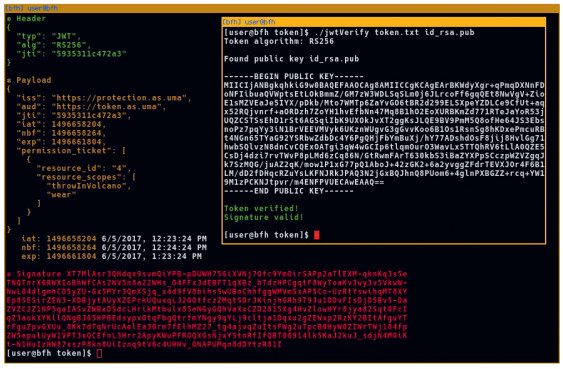
Conclusion

As UMA is built upon OAuth 2.0 it inherits its characteristics – the good, the bad and the ugly. From our point of view UMA seems to be very robust and adaptable for various use cases and we found only minor issues regarding the different tokens and their security properties and thus we can provide recommendations for further implementations.



Jérôme Jamin

Benjamin Stauffacher



UMA Permission Ticket