Digital Verification Advancements at RWoT III

An Overview from Rebooting the Web of Trust III Design Workshop

by Manu Sporny with Christopher Allen, Harlan Wood, and Jason Law

There were a number of enhancements made to Digital Verification at the 3rd Rebooting Web of Trust event. The following document summarises the advancements made as a direct result of participation from the workshop attendees.

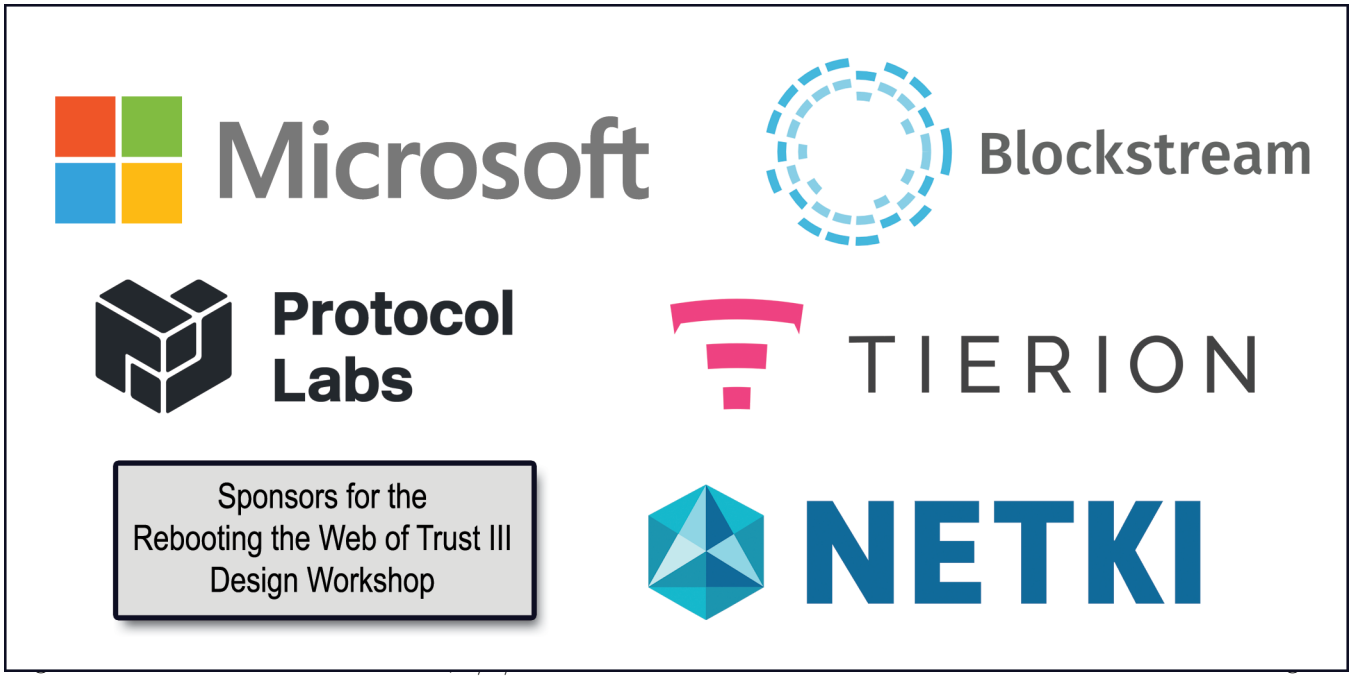
FOUNDING OF THE W3C DIGITAL VERIFICATION COMMUNITY GROUP

Based on various hallway and lunch discussions, it became evident that the community wanted a more permanent location to store artifacts and work on them. As a result of these discussions, the W3C Digital Verification Community Group was proposed, supported, and formed. Anyone may join the group by going to the following URL and clicking the "Join" button:

https://w3.org/community/digital-verification/

The following specifications were migrated from the Web Payments Community Group to the Digital Verification Community Group:

- Linked Data Signatures
- RSA 2016 Linked Data Signature Suite
- Koblitz 2016 Linked Data Signature Suite
- Pseudonymous 2016 Linked Data Signature Suite



AUTHORING THE VERIFIABLE CLAIMS SPECIFICATION PRIVACY AND SECURITY SECTION

A group was convened to discuss the privacy and security considerations for the Verifiable Claims Data Model and Representations specification. The considerations were documented and integrated into the Verifiable Claims specification, which can be found at the following link:

https://opencreds.github.io/vc-data-model/

CREATION OF KOBLITZ 2016 SIGNATURE SUITE SPECIFICATION

The Koblitz 2016 Signature Suite was discussed, implemented, and formalized in a Signature Suite specification designed as an extension to the Linked Data Signatures specification:

http://w3c-dvcg.github.io/lds-koblitz2016/

CREATION OF PSEUDONYMOUS 2016 SIGNATURE SUITE SPECIFICATION

A pseudonymous signature suite based on the Camenish-Lysyanskaya signature mechanism was discussed and formalized in a Signature Suite specification designed as an extension to the Linked Data Signatures specification:

http://w3c-dvcg.github.io/lds-pseudonymous2016/

ADDITION OF MULTI SIGNATURE AND CHAINED SIGNATURE SUPPORT

A number of hallway discussions led to the general requirements and finalization of the design for multi-signature and chained signature support in the Linked Data Signatures specification:

http://w3c-dvcg.github.io/ld-signatures/ - multiple-signatures

Additional Credits

Lead Paper Editor: Manu Sporney

Contributors: Christopher Allen, Harlan Wood, Jason Law

About Rebooting the Web of Trust

This paper was produced as part of the **Rebooting the Web of Trust III** design workshop. On October 19th through October 21st, 2016, over 40 tech visionaries came together in San Francisco, California to talk about the future of decentralized trust on the internet with the goal of writing 3-5 white papers and specs. This is one of them.

Workshop Sponsors: Blockstack, Microsoft, Netki, Protocol Labs, Tierion

Workshop Producer: Christopher Allen

Workshop Facilitators: Christopher Allen and Brian Weller, additional paper editorial & layout by Shannon Appelcline, and additional support by Kiara Robles and Marta Piekarska.

What's Next?

The design workshop and this paper are just starting points for Rebooting the Web of Trust. If you have any comments, thoughts, or expansions on this paper, please post them to our GitHub issues page:

https://github.com/WebOfTrustInfo/rebooting-the-web-of-trust-fall2016/issues

The next Rebooting the Web of Trust design workshop is scheduled for Spring 2017 in Paris, France. If you'd like to be involved or would like to help sponsor these events, email:

ChristopherA@LifeWithAlacrity.com