# VC-ZKLang

## Specification of Privacy-Enhancing Implementation of Verifiable Claims

Jan Camenisch Manu Drijvers ?

30th November 2017

**Abstract**

This document specifies an language that allow one to describe the cryptographic protocols that will generate a cryptographic token as a witness to a verifiable claim. The cryptographic protocol that will then be executed from this specification should be (but need not be) such that the token is not linkable to the credentials on which it is based.

## Contents

# 1 ZKLang

If credentials are key-bound, they are required to be bound to the same (secret) key.

At this level, all message $m_i$ are integers. Terms that the language supports are the following ones.

$$\text{NIZK}\{(m_i)_{i\in h}[m]_{i\notin h} : \text{Credential}(\mathit{issuer\_public\_key}, m_1, m_2, m_3)\} \quad (1)$$
$$\text{NIZK}\{() : \text{Nym}(\mathit{nym})\} \quad (2)$$
$$\text{NIZK}\{() : \text{SNym}(\mathit{nym}, \mathit{scope})\} \quad (3)$$
$$\text{NIZK}\{(m) : \text{Enc}(\mathit{epk}, m, \mathit{ctxt})\} \quad (4)$$
$$\text{NIZK}\{(m) : \text{Larger}(m, c)\} \quad (5)$$
$$\text{NIZK}\{(m) : \text{Smaller}(m, c)\} \quad (6)$$

Example composition of a statement.

$$\begin{aligned}\text{NIZK}\{(m_1, m_2, m_3, m_4)[m_5] :\ & \\ & \text{Credential}(\mathit{ipk}_1, m_1, m_2, m_3) \ \wedge\ \text{Credential}(\mathit{ipk}_2, m_1, m_4, m_5) \ \wedge \\ & \qquad\qquad \text{Nym}(\mathit{nym}) \ \wedge\ \text{Larger}(m_3, c)\}\end{aligned}$$

Explanations of stuff

# 2 Mapping Verifiable Claims to ZKLang

This mapping will depend on the credential specification of the issuer of a credentials.

## 2.1 Mapping the different types to integers

## 2.2 Age proof

## 2.3 Membership proof

# 3 Realization of ZKLang Components

We could do all of this with X509 credentials, but then have no privacy features. We here concentrate on how to do this with the privacy features.

$m_i$ from $Z_q$, so everything in prime order group
Nyms
CL sigs
Vereng
Orchestration