

Digital Identity & the Public Sector

Using verifiable credentials to manage social security

October 3, 2023

Trevor Butterworth

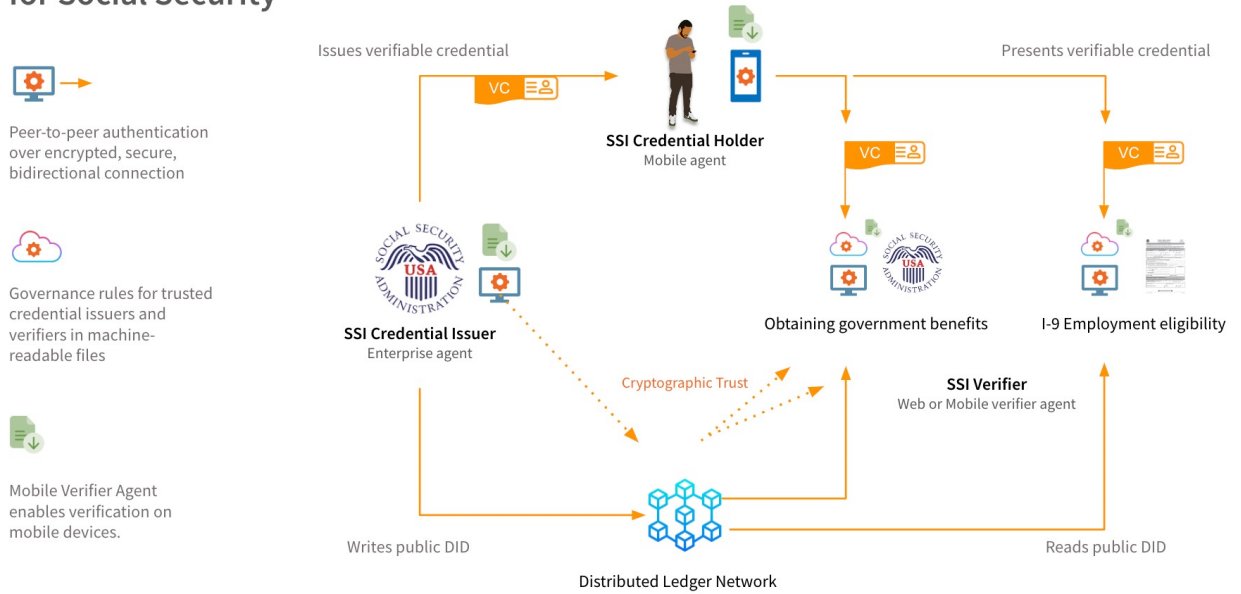
Overview

Issuing a verifiable credential for a Social Security Number (SSN#) would provide a frictionless, fraud-resistant way to manage benefit and employment applications and to interact with other federal and state government services.

Using a verifiable credential for Social Security Numbers also presents an opportunity to fix a major weakness in systems that rely on the number alone: Using a SSN# as both an identifier *and* a security mechanism means that knowing the number is often enough to gain access to sensitive data or privileges.

By requiring the SSN# to be presented *in* a verifiable credential, knowing the number will not be enough to compromise security.

A Trusted Digital Ecosystem for Social Security



Indicio

Copyright 2023 Indicio PBC

Workflow: Issuing a Verifiable Social Security Card Credential

The Social Security Administration will first create a digital schema to issue verifiable social security card credentials. With only a single write to a distributed ledger network, the schema will describe the structure of every social security card, including the attribute fields it must contain. The ledger data will also link this schema to the Administration issuing the verifiable credential. No personal data has been written to the ledger; this is just a template that will be used by Social Security Administration offices to issue a SSN# directly to an individual.

After a person has passed the normal identity assurance process at a Social Security Administration Office, and they are ready to receive a physical card, the office will also offer a verifiable credential for their SSN#. This can be done in a variety of ways, depending on whether the person has a mobile device or not.

Assuming they have a mobile device, they can scan a QR code that establishes a direct connection with the Social Security Administration (this may require a prompt to the person to download a digital wallet with the appropriate software to manage the connection).

Indicio

Once a secure, bi-directional connection has been established, the person will be offered their Social Security Card as a verifiable credential. If they accept, they will receive a credential populated with their specific number. Only the Social Security Administration Office and the person who has just received the verifiable credential hold the Social Security data. This number is not written to the ledger.

All this can take place in the Social Security Administration Office. Biometric binding and liveness check requirements to both the device and the software for managing the credential can be used to ensure the device and software cannot be used by someone else.

Workflow: Verifying a Verifiable Social Security Card Credential

The power of verifiable credentials to authenticate data draws on the simplicity of combining the cryptographic trust of a credential, proof of data integrity, and ease of verification through simple, mobile software.

A verifiable credential can be verified anywhere — for example, it can be verified in parallel with a phone conversation so that an office could authenticate a legitimate card holder over the phone—and the technology is currently being developed to enable offline verification.

When a person presents their Social Security Card Credential for, say, a job application, the employer uses either desktop or mobile verifier software to request a presentation of the person's credential data (i.e., their SSN#). The combination of public key infrastructure (cryptographic trust), digital signatures (the integrity of the attribute field and the SSN#), and the published and known governance of the Social Security Administration, prove the source of the credential and the integrity of the SSN#.

This all happens instantly.

The ability to instantly verify the authenticity of government-issued identity in a way that cannot be forged, guessed, or stolen provides a powerful way to mitigate fraud across multiple domains, and one that can scale easily to the level of a population.

To learn more about Indicio's award-winning verifiable credential solutions or see a demo, [CONTACT US](#)