

The Case for a New Social Authentication Era

Jean Martina, Larissa G. Rosa and Gustavo Zambonin

Federal University of Santa Catarina

October 13, 2026

The Problem

There is a need to rethink authentication methods to align them with the demands and technological realities of 2025

- ▶ The internet is less trustful, **it is increasilly easy to pretend that you are someone else** from the real world;
- ▶ **Password-based authentication** is vulnerable to attacks, example: brute force;
- ▶ **Biometric methods** face new risks with AI advancements;
- ▶ **Storing keys on personal devices** can lead to access issues if the device is lost or stolen.

Social Authentication as a Solution

- ▶ Traditional authentication methods (passwords, devices, biometrics) may no longer be sufficient to prove our real-world identity or confirm our online actions;
- ▶ In such cases, turning to someone we know for verification becomes a natural alternative.

A Promising Idea That Struggled to Take Off

- ▶ **Early Proposals:** The concept was introduced years ago but never gained widespread adoption;
- ▶ **Limited Use Cases:** Where implemented, social authentication is often linked to security vulnerabilities.

What went wrong? Can we fix it?

What went wrong?

- ▶ **Easy Access to Personal Data:** Knowledge-based social authentication, like Facebook's picture-based recovery, is weak because attackers can easily gather needed information from social networks;
- ▶ **Single Point of Failure:** Vouch-based authentication often relies on a single trusted contact, making it vulnerable if that contact is compromised or unavailable;
- ▶ **Outdated Contact Lists:** Users rarely update their trusted contacts, meaning their authentication network may not reflect their current social relationships;
- ▶ **Authentication Distance:** Trust-based authentication may fail when contacts are geographically distant or unavailable at the time of verification.

What should social authentication have?

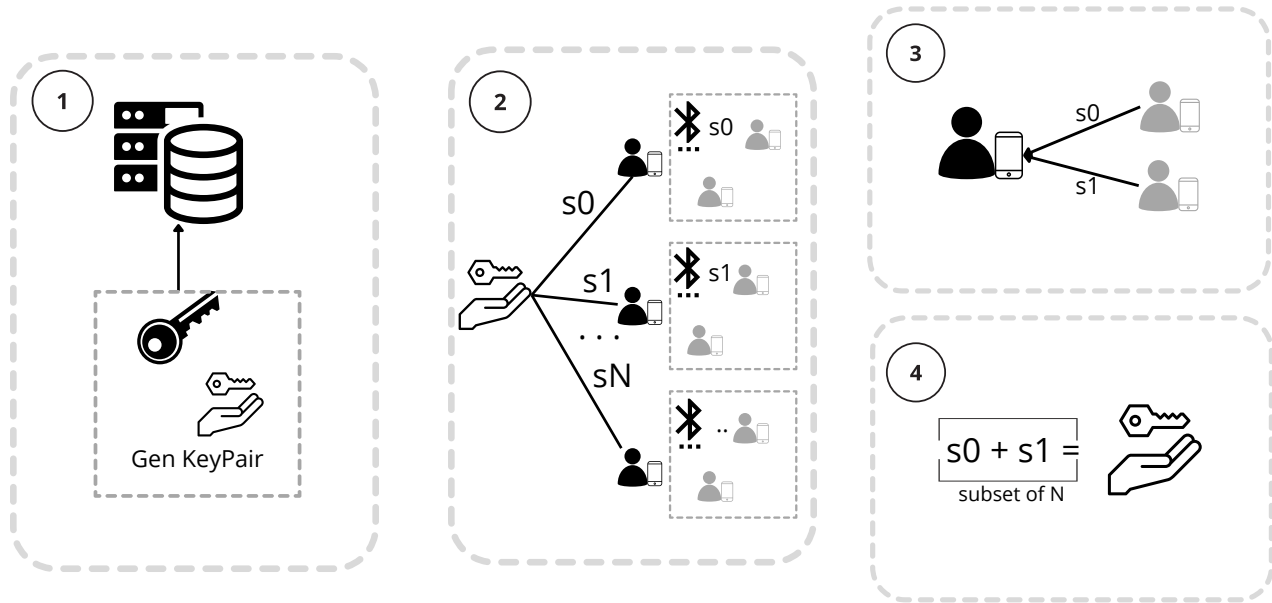
- ▶ **Ideal Social Authentication:** Should update security contacts automatically, ensure fast responses, and maintain privacy (in the sense that we don't want to leak our contacts to the internet).
- ▶ **Avoiding Known Issues:** Must not rely on easily accessible data (knowledge-based) or constant human intervention.

Should we always use it?

We should use it to leverage the credibility of a known individual based in the society around them. Examples:

- ▶ SIM Swap attack;
- ▶ Automatic identity management on companies;
- ▶ Prove your actions, like posts, were made by you (deepfake problems).

Possible Solution



The following example illustrates the process of updating trustee contacts in the absence of any deliberate initiation of the flow by a human.

Discussion

- ▶ We are looking for a formalization of this model applied in the SIM Swap case, as well as what properties it should have;
- ▶ Is it feasible to develop a generic model to cover other cases?

Could a system that mimics or understands the real social fabric, even if only in the context of authentication, foster collaborative benefits?

The end

Thank you for your time