



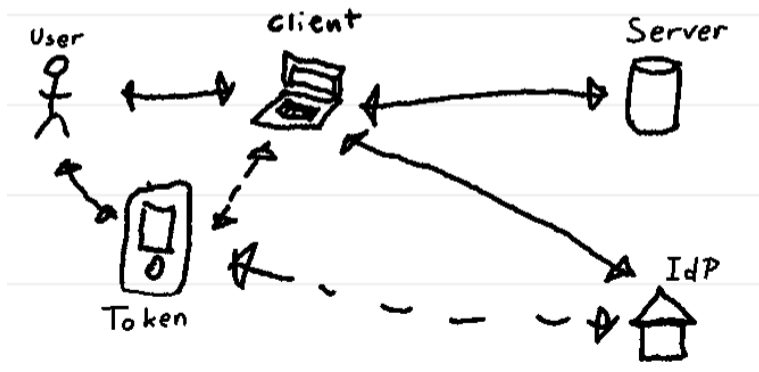
Modeling User Mistakes in eID

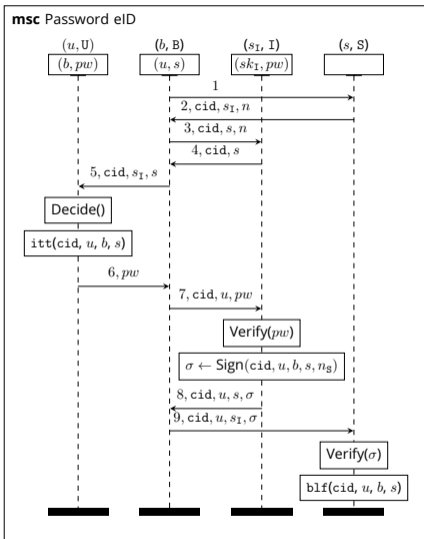
Ole Martin Edstrøm
October 30, 2025

What is an eID

eID - "Definition"

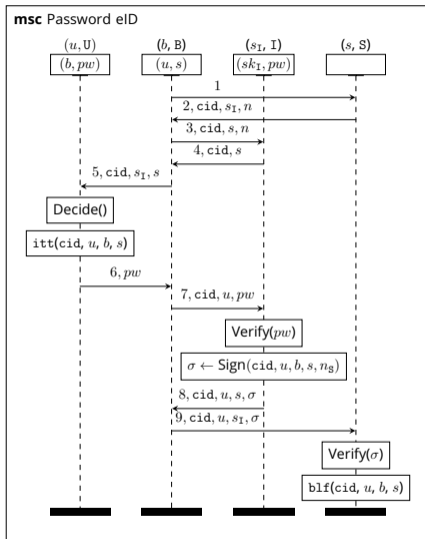
In a generic way, an "Electronic identity" is a means for people to prove electronically that they are who they say they are and thus gain access to services.





How do we model eIDs

- ▶ We start with a set of *Roles* and a set of *Agents*.
- ▶ All eIDs has the roles *User*, *Browser* and *Server*.
- ▶ How to define security
 - ▶ Set of *Intents* from the users.
 - ▶ Set of *Beliefs* from the servers.
 - ▶ The eID is secure if the set of intents contain the set of beliefs.



Honest Users Makes Honest Mistakes: A Framework for Analyzing eID Protocols

By: Ole Martin Edstrøm, Kristian Gjøsteen, Hans Heum, Sjouke Mauw and Felix Stutz

On ePrint: <https://eprint.iacr.org/2025/1686>

- ▶ In this paper, we formalized this model.
- ▶ With this model we used Tamarin to study 15 different Protocols, each in 4 different scenarios.
 - ▶ With Perfect and imperfect users
 - ▶ With Honest and Corrupt browsers.

Results from Tamarin

User browser tabs	honest & corrupt		all honest	
	imperfect	perfect	imperfect	perfect
Password	x	x	x	✓✓✓✓
App	✓	✓	✓	✓
App ⁺	✓	✓✓	✓	✓✓
App Cmp	✓	✓	✓	✓✓✓
App Cmp ⁺	✓	✓✓✓	✓	✓✓✓
App Write	✓	✓	✓	✓✓✓✓
App Write ⁺	✓	✓✓✓	✓	✓✓✓✓
Two-factor	✓	✓	✓	✓†
Two-factor ⁺	✓	✓✓	✓	✓✓†
Two-factor Cmp	✓	✓	✓	✓✓✓
Two-factor Cmp ⁺	✓	✓✓✓	✓	✓✓✓
Two-factor Write	✓	✓	✓	✓✓✓✓
Two-factor Write ⁺	✓	✓✓✓	✓	✓✓✓✓
WebAuthn	✓	✓	✓✓✓	✓✓✓✓
WebAuthn ⁺	✓	✓✓✓	✓✓✓	✓✓✓✓

Tank You!