CERIAS

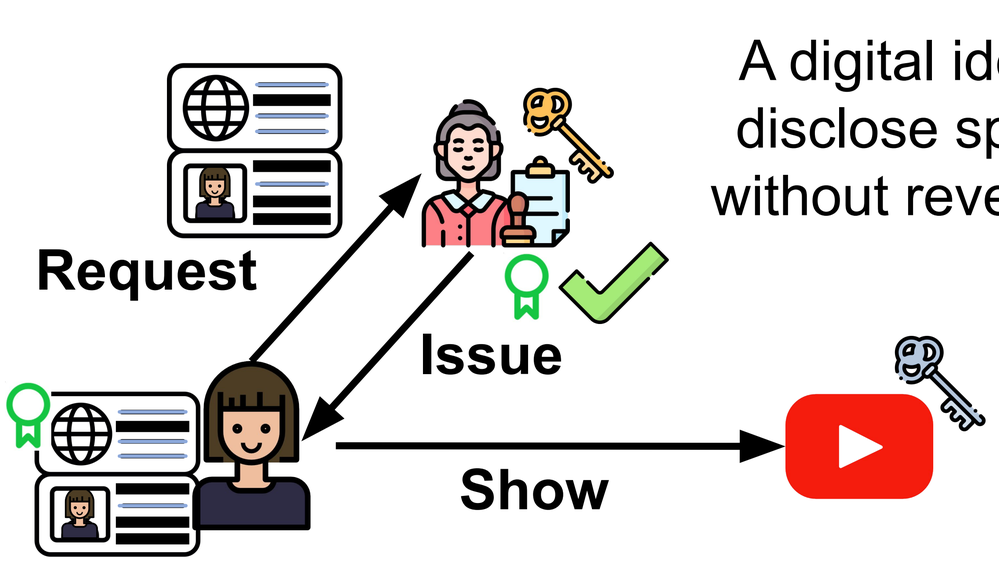
The Center for Education and Research in Information Assurance and Security

`zk-creds`: Flexible Anonymous Credentials from zkSNARKs and Existing Identity Infrastructure

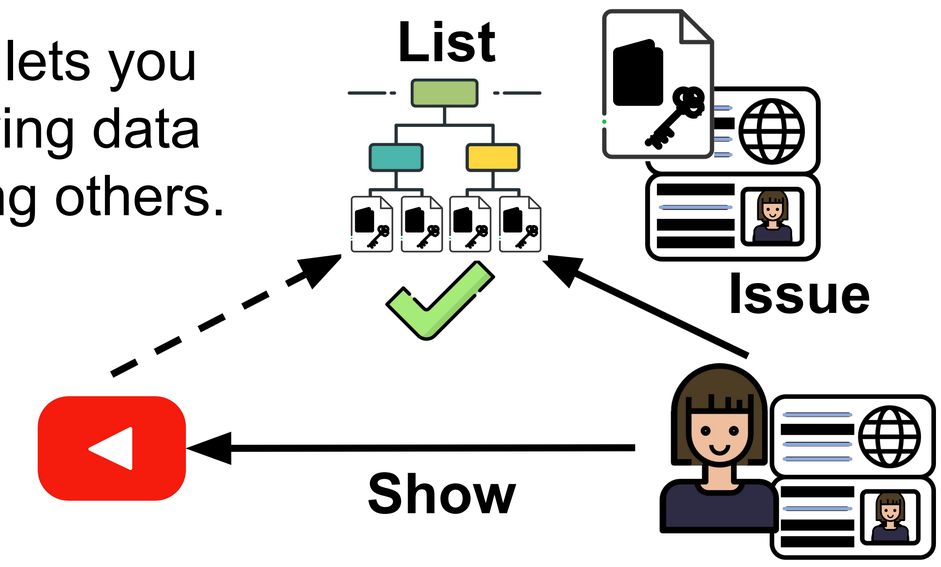
Michael Rosenberg, Jacob White, Christina Garman, Ian Miers

{white570,clg}@purdue.edu {micro,imiers}@umd.edu

What is an Anonymous Credential?

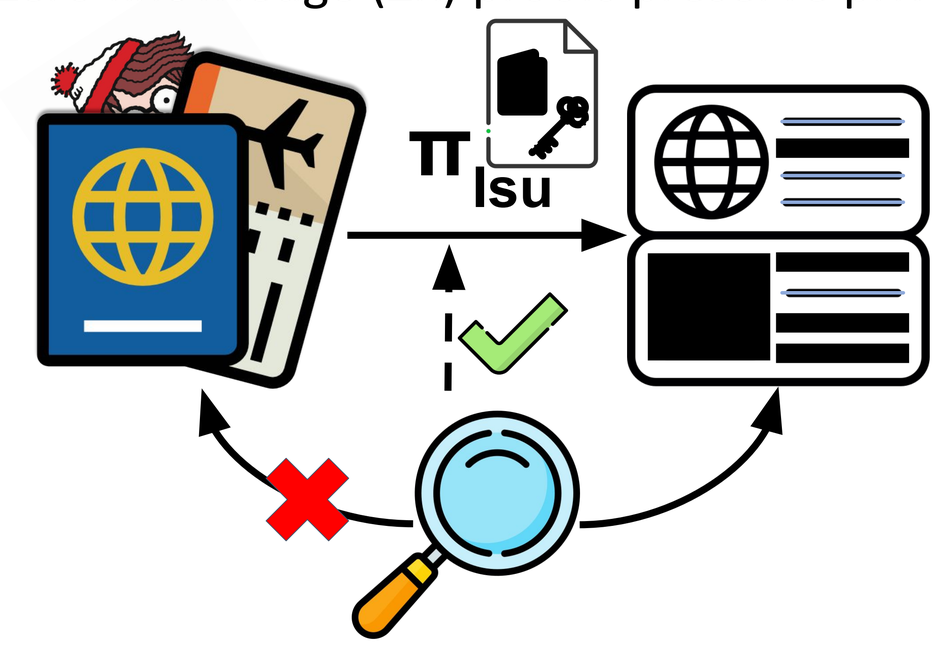


A digital identifier which lets you disclose specific identifying data without revealing or linking others.



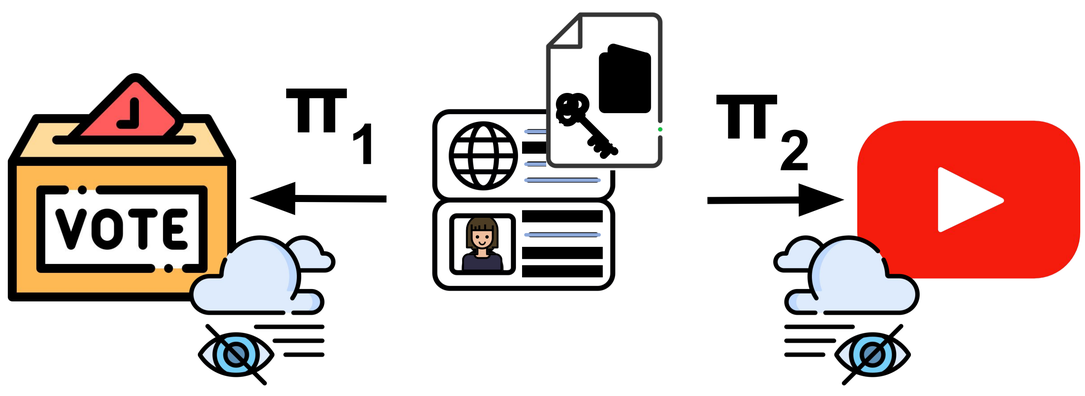
Decoupling ID Assurance from Issuance

- Minimize burden of authorizing anonymous credentials & using customized cryptography
- Bootstrap from trusted identity documents
- Zero knowledge (ZK) proofs preserve privacy



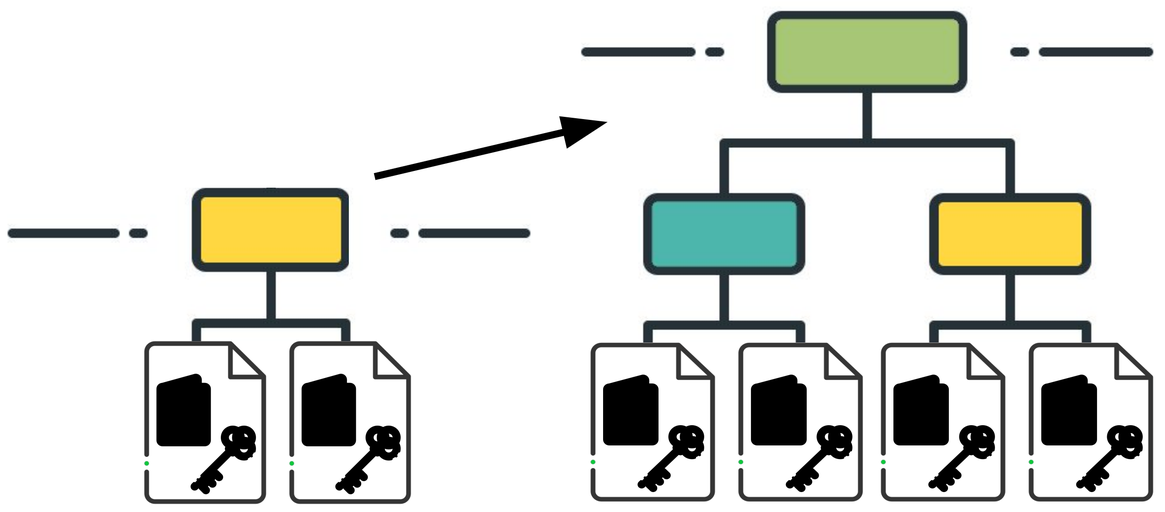
Complex & Composable Statements

- Leverage rich zkSNARK proof framework
- Gadgets: rate limiting, anti cloning, expiry, etc.
- Unlinkable shows of credential between apps



Flexible & Auditable Issuance

- Auditable, verifiable issuance of ZK credentials
- Multi issuer, multi application interoperability
- Efficient, dynamic additions to membership list
- Privacy aware list publication and updates



Efficient & Open Source Libraries

- User friendly anonymous credentials API
- Combine & reuse slow proofs (e.g. membership)
- < 150 ms to show, < 5 ms to verify, ~ 1 KB proof size

	IssueReq	IssueGrant	ShowCred	ShowCred (full)	VerifyShow
Age-restricted vid.	1.97s	2ms	143ms	602ms	5ms
Entering a bar	1.97s	2ms	98ms	557ms	5ms

Client-opt. (C) / **Server-opt. (S)**	ShowCred C	ShowCred C (full)	ShowCred S	VerifyShow C	VerifyShow S	VerifyShow S (batch)	Proof Size C	Proof Size S
Simple Possession	5ms	465ms	450ms	3ms	1.5ms	1.8 verifs/ms	744B	192B
Expiry	53ms	526ms	461ms	5ms				
Linkable Show	43ms	494ms	457ms				1064B	
Rate Limiting	60ms	507ms	461ms					
Clone Resistance	90ms	542ms	530ms					

PURDUE UNIVERSITY

Presenter: Jacob White

PI: Dr. Christina Garman

GitHub: rozbb/zkcreds-rs

CERIAS