

ADAPID E-GOVERNMENT APPLICATION:

PRIVACY-ENHANCED
E-PETITIONS

Claudia Diaz

COSIC – K.U.Leuven

2nd ADAPID Workshop
28/09/2007

Petitions in the physical world

- ▣ Formal request addressed to an authority and signed by numerous individuals
- ▣ Typically citizens provide
 - Unique identifier (name, national ID number)
 - Signature
- ▣ Verification:
 - Validating that the signatures correspond to the identifiers
 - Discarding multiple/invalid signatures

Electronic petitions

- ▣ Benefits of going electronic:
 - ▣ Many resources are needed in order to physically collect the signatures
 - ▣ Manual signature verification is a costly and tedious process
- ▣ Good example of ICT enabling participatory *e-democracy*
- ▣ Electronic petitions have technically challenging requirements that make it an interesting application

The naive e-petition implementation

- ▣ Have users sign the petitions with their e-ID
 1. Select petition
 2. Sign using the e-ID (2-factor authentication)
 3. Check that the petition has not yet been signed with that e-ID
 4. Count (or discard) the signature
- ▣ Privacy risks
 - Leak sensitive information on political beliefs, religious inclinations, etc.
 - Through unique identifiers, petition signatures can be linked to other data

e-petition requirements

- ▣ Basic requirements
 - Authentication: citizen is who claims to be (i.e., no impersonation)
 - Required attributes: citizen is entitled to sign (e.g., age > 18)
 - Uniqueness: citizens sign a petition only once
 - Correctness: all valid signatures are counted
- ▣ Privacy requirements
 - Citizen unlinkable to petition (i.e., not possible to identify *who* are the signers)

Anonymous credential protocols

- ▣ Active area of research in cryptography
- ▣ They rely on cryptographic protocols and Zero-Knowledge proofs to reduce to the bare minimum the amount of information disclosed
- ▣ Flexible protocols, many options possible
- ▣ Example:
 - CI issues a credential to U that encodes U 's age
 - U can prove to V that his age is above/below a threshold
 - V does not learn U 's exact age
 - V can check that this is certified by CI

PKI vs anonymous credentials

PKI

- Signed by a trusted issuer
- Certification of attributes
- Authentication (secret key)
- Double-signing detection

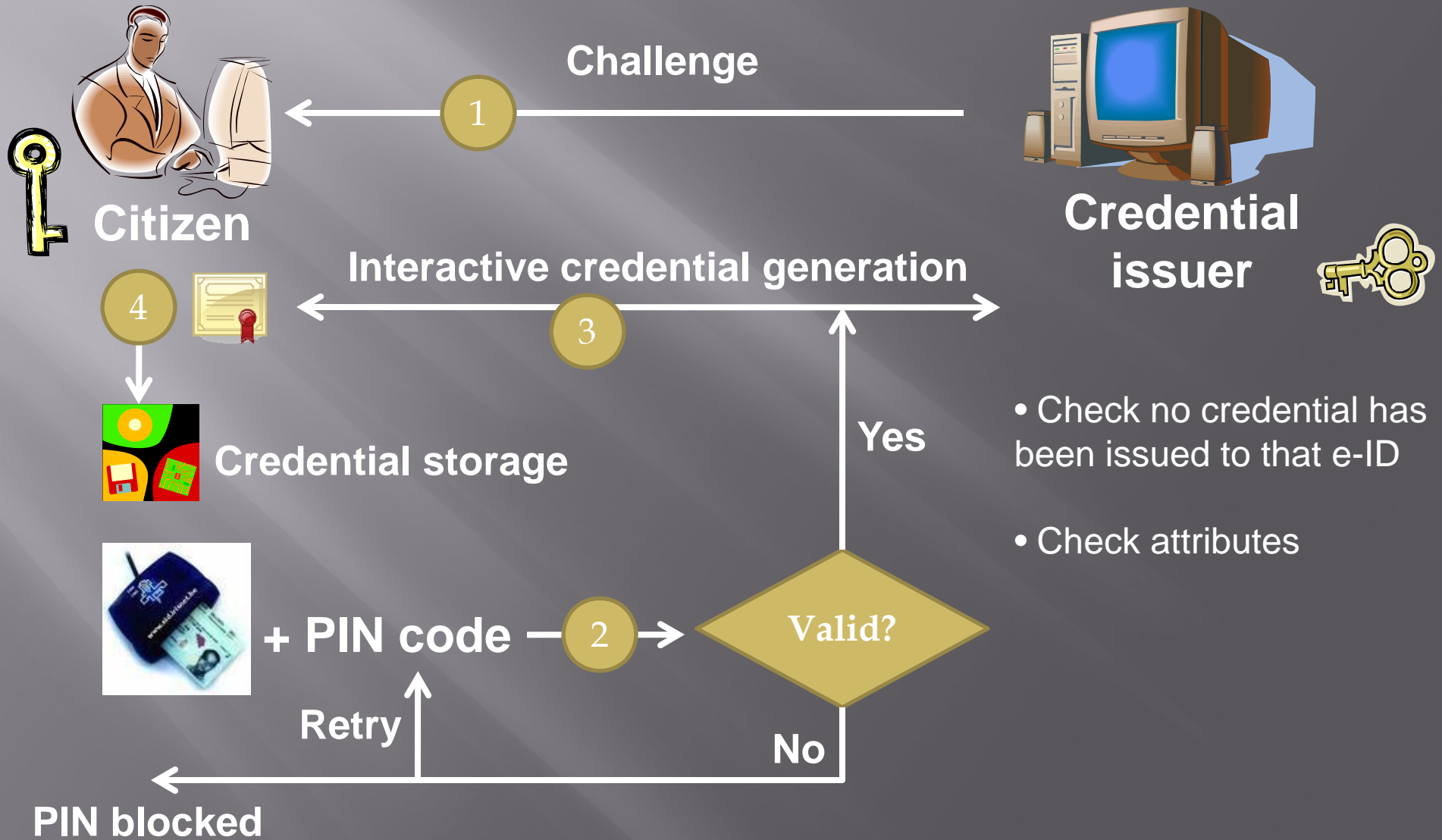
- No data minimization
- Users are identifiable
- Users can be tracked (Signature linkable to other contexts where e-ID is used)

Anonymous credentials

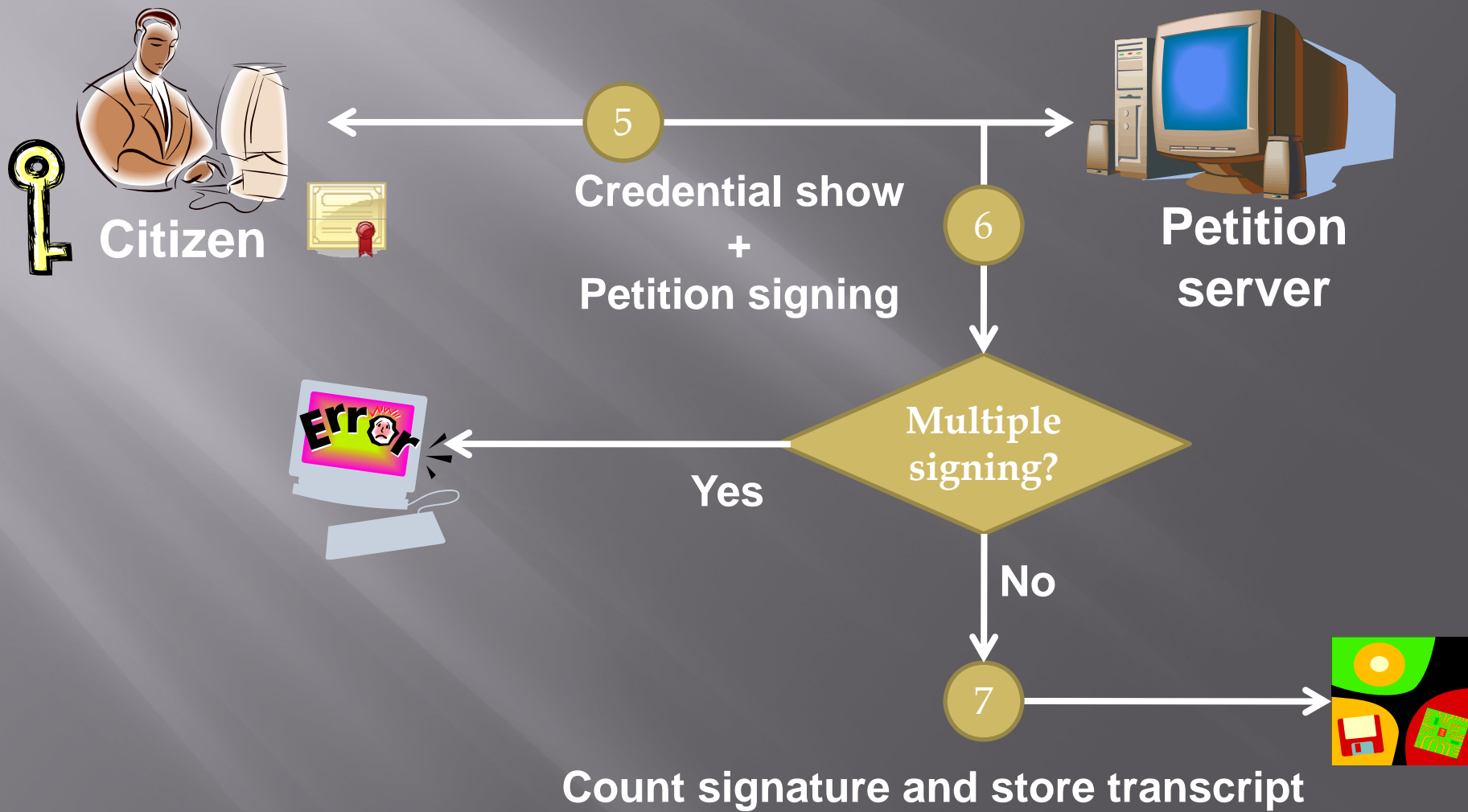
- Signed by a trusted issuer
- Certification of attributes
- Authentication (secret key)
- Double-signing detection

- Data minimization
- Users are anonymous
- Users are unlinkable in different contexts

Protocol 1: obtaining a credential



Protocol 2: signing the petition



Properties

- ▣ Only citizens entitled to sign can do so
 - Possession of e-ID + knowledge of PIN
 - Attribute verification (e.g., age, locality)
 - One credential per citizen
- ▣ Citizens can sign only once (multiple signing is detectable so that repeated signatures can be deleted)
- ▣ Collusion of credential issuer and e-Petition server does not reveal the identity of a signer

Demonstrator

- ▣ Implemented in Java
- ▣ Components:
 - E-ID card, car reader and middleware
 - SSL/TLS client-server communication
 - Anonymous credential protocols (extension of currently available primitives provided by Idemix)
 - Graphical user interfaces
- ▣ Proof-of-concept
 - Security with lowest required level of identification
 - e-ID can be used to bootstrap secure and privacy friendly identity management

Open issues

- ▣ Improved implementation
- ▣ Allow citizens to add petitions
- ▣ Secure storage for the user master secret
- ▣ Prevent timing and traffic analysis attacks

Summary and conclusions

- ▣ Motivated the choice of e-petition applications
- ▣ Combined and extended various building blocks to implement privacy-enhanced e-petitions
- ▣ Overview of protocols and properties
- ▣ Security properties can be achieved without identifiability

Thank you!

